CHAPTER

1

WINDOWS 2000 NETWORK INFRASTRUCTURE OVERVIEW

After reading this chapter and completing the exercises you will be able to:

- Describe the basic elements of networking
- Describe the various Physical and Data Link layer protocols and technologies
- Define the differences among the five network connectivity models
- Explain the Windows 2000 TCP/IP protocol and services

Welcome! We're delighted that you've chosen to learn about designing a Windows 2000 network infrastructure. Whether you're a network professional looking to add a new skill set or a student working on passing an MCSE exam, you will find this book good preparation for the tasks ahead.

Before we delve into the art and science of design, we devote this chapter to summarizing the protocols and services surrounding the subject of design. This is done for the same reason that an apprentice craftsman would take an inventory of his tools before attempting to build a piece of furniture. If after reading this chapter you find you're a bit rusty on some of the topics, please visit www.course.com to find resources that you can use to refresh your skills.

Note that knowledge of most of the following protocols and services is assumed to be a prerequisite of this course. Therefore, most of this material is presented only as a review.

Networking Basics

We begin “from the ground up” with a review of the network environment and the **Open Systems Interconnect (OSI) reference model**. This basic knowledge will help you to understand the networking components and their dependencies in order to create a usable design. It will also come in handy when you are troubleshooting; one effective strategy for troubleshooting is to start at the bottom of the OSI reference model and work your way up. You’ll use a test environment during an actual design that will give you plenty of opportunities for troubleshooting.

Networks Take Their First Steps

A network can be as simple as two or more computers connected to communications **network media** for the sake of sharing data and other resources, such as printers or modems. Today this medium can be copper wire, fiber-optic cable, or a wireless technology based on radio waves, microwaves, or even infrared.

Computer networks were born in the 1960s, when research institutions and government agencies needed to connect to and share the computing power of very large, expensive mainframe computers. They used simple “dumb” terminals (teletypes, Friden Flexowriters, etc.) that were hooked up to telephone and telegraph lines and connected to specialized interfaces attached to the mainframe.

However, a major shift occurred in the late 1970s—personal computers from Radio Shack and Apple started to appear in homes, schools, and even offices. These PCs could be used as “smart” terminals to connect to computer centers. CRT terminals were coming into use prior to the personal computer, but they generally were very limited in their abilities. The advent of the IBM PC in 1981 and the development of more and more business software gave credibility to the personal computer as a business tool. It was only a matter of time before we would want to connect these PCs.

This was when most of us who were supporting computers first started using the term **local area network (LAN)** to describe networked computers and shared resources that are physically close to one another, as in a single office or floor or building. In spite of their inauspicious beginnings, LANs improved and made their way into businesses, government agencies, colleges and universities, and other organizations in the ’80s and ’90s. It wasn’t long before people wanted to connect LANs to each other. Devices and software were developed to support these connections, and we now call connected LANs that span a city or metropolitan area a **metropolitan area network (MAN)**. When connected LANs span a greater geographical area—from city to city, for instance—we call that a **wide area network (WAN)**. The **Internet** is the biggest example of a WAN, comprising thousands of LANs and MANs worldwide.

The OSI Reference Model

Networking components and **protocols** are often described as functioning within the physical and logical layers of the OSI reference model, as defined in the 1970s by the International Organization for Standardization (ISO). (Yes, these names and acronyms are confusing! It gets worse.) This model was created by the ISO to categorize the necessary functionality for communication between computers. It is not tied to any government or vendor, but rather is a model that describes the functions that they predicted would need to be performed for computers to communicate within networks.

Note

For more information about the ISO, refer to Hands-on Project 1-1.

The OSI reference model is a layered model, implying that hardware and software components at each layer perform specific tasks that, when taken together, enable data to be transmitted and received over a network. The components at each layer provide services to the layers above them.

The layers are, from bottom to top, Physical, Data Link, Network, Transport, Session, Presentation, and Application. They are numbered from bottom to top (1 through 7), and they are often referred to by their numbers. For example, a layer 2 switch operates at the Data Link layer. Although current network technologies do not strictly map to the seven-layer model, it is still used to describe network components and functions, as shown in Figure 1-1.

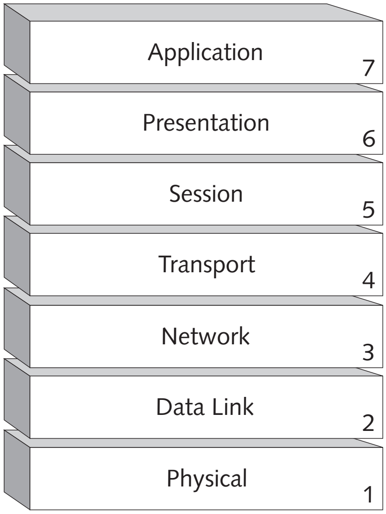

Figure 1-1 The OSI reference model

According to the OSI reference model, each layer performs a certain set of functions. This layering of protocols is often referred to as a "stack," as in the **Transmission Control Protocol/Internet Protocol (TCP/IP)** stack. As shown in Figure 1-2, the protocols at each layer on the sending end act as if they are communicating with the corresponding, or peer, protocols on the receiving end. On the sending end, beginning at the Application layer, the data and appended information are passed down "vertically" through the layers, with additional information being added at each layer. On the receiving end, the components at each layer act on the information from the peer protocol on the corresponding layer of the sending computer, in effect, peeling off its information.

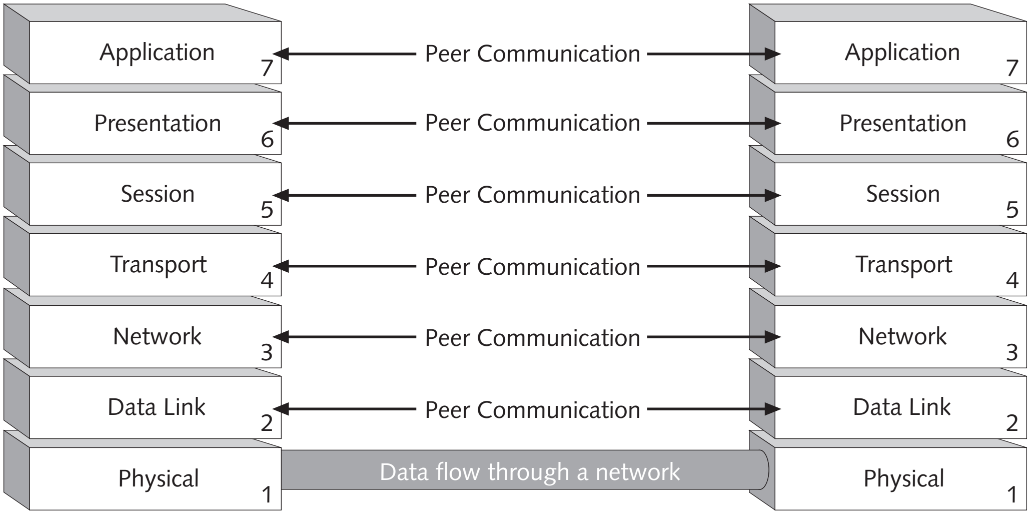

Figure 1-2 Network layer peer communication

Working our way through the layers, beginning at the top, we see a journey of information from one computer to another. First, a user, through an end-user application such as a word processor or the client side of a client/server application, makes a request for data on the network. This request is processed through a standard set of interfaces, or **Application Programming Interfaces (APIs)**, at the network **Application layer**. This top layer provides the user interface, giving users access to the network, providing file access and transfer services, mail transfer services, terminal emulation services, and directory services, as well as network management and other network services.

The Microsoft Windows Redirector is an example of a program that works at the Application layer. In Windows 2000, another Application layer protocol is the Common Internet File System (CIFS). This name may be new, but it is not new to Windows—it was part of Windows NT Service Pack 3. CIFS is the next generation of Server Message Protocol, the file- and print-sharing protocol of Microsoft networking. CIFS in Windows 2000 includes new features while maintaining backward compatibility with previous versions of Windows. Although some Application layer protocols, such as FTP and TFTP, allow file read or transfer capabilities, CIFS supports simultaneous read/write file access. It also supports many of the newer features of Windows, such as Distributed File System, file and record locking, file change notification, and read-ahead and write-behind operations. All of these features are supported over any IP-based network.

Note

API is a set of interfaces (now frequently in the form of an Object Model) that a software company publishes so that third parties can develop custom extensions to their software. Programs at each layer of the OSI model exchange data or instruct each other to do something via APIs.

The resulting data, the user's request in this case, are referred to as a message and sent down to the **Presentation layer**, where formatting of the data and any necessary data conversions are done. In addition, the Presentation layer handles data compression, data encryption, and data stream redirection. As with other layers, the Presentation layer adds its own control information as a header to the data received from the Application layer.

Next, the **Session layer** manages the session between two computers, working to establish, synchronize, maintain, and end each session. Authentication, connection ID, data transfer, acknowledgments, and connection release are performed by the protocols at this layer. This layer treats the combined data and header received from the Application layer as data and adds its own header. Figure 1-3 shows headers added at each layer. Headers are shown with a subscript to indicate the order in which they are added. After a header is added, the next layer treats the previous layer's header as data and adds its own header.

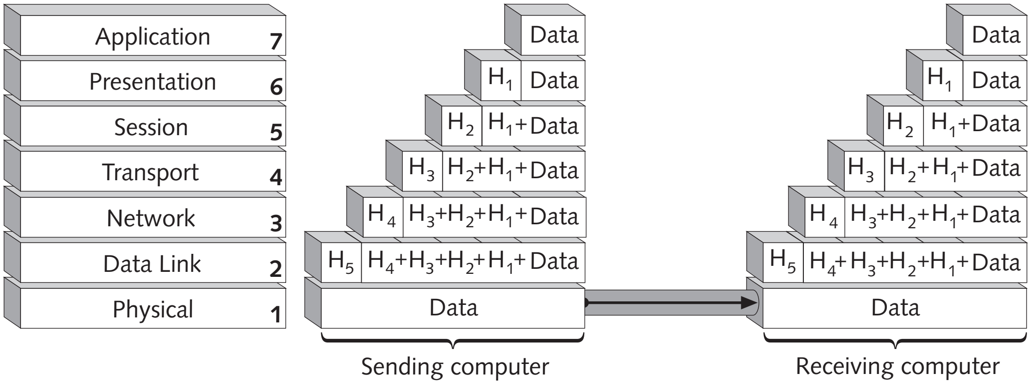

Figure 1-3 OSI reference model headers

The **Transport layer** is responsible for error and flow tracking, dividing outgoing messages into smaller segments, and reassembling incoming messages. The Transport layer adds its own header to the segment. Transport Control Protocol (TCP) and Sequenced Packet Exchange (SPX) are Transport layer protocols of TCP/IP and IPX/SPX, respectively.

The **Network layer** provides the logical addressing scheme for the network, uniquely identifying devices across the entire network. The segments from the Transport layer receive their logical addresses and are referred to as **packets** or datagrams. This logical address is very important in routed networks. Network layer protocols are broken into two categories: routed (for example, TCP/IP and IPX) and nonrouted (for example, NetBEUI and SNA). Both routed and nonrouted protocols uniquely identify devices on a network. The difference is that the scope of a routed protocol goes beyond the single broadcast domain of a nonrouted protocol. The nonrouted protocols have no notion of a unique subnet address, whereas the routed protocols uniquely identify a device across an entire internetwork, or internet for short.

Note

Notice the lowercase "i" in internet. The Internet is just one of many internets. Although somewhat confusing, the terms "network" and "internetwork" are used to describe technical concepts, while "intranet," "Internet," and "extranet" are used to describe the organization or application of networks and internetworks. Put another way, a "network" could be part of an "intranet" or "extranet," depending on what you use it for.

When working with a **protocol stack** that includes logical addresses, such as TCP/IP and IPX/SPX, we have both the routed protocols described above and the routing protocols. The routed protocols provide the logical addresses, and these addresses are used by routing protocols, such as Routing Information Protocol versions 1 and 2 (RIP v1 and RIP v2) and Open Shortest Path First (OSPF). Routing involves forwarding packets from one subnet to another, based on the logical address. The routing protocols use the destination address in a packet to determine how to route the packet to the subnet where the destination computer resides.

A router that has routing software capable of routing IP packets is called an "IP router." This can be a dedicated router, such as a Cisco or 3Com router, or a server, such as Windows NT or Windows 2000 with routing capabilities enabled.

The routing protocols and services prevent network congestion while routing data from source to destination. In addition to directing traffic, features implemented in various devices use Network layer information to block **broadcast** traffic (packets addressed to a special address, meaning "all hosts") and optionally other identifiable traffic. However, the logical addressing of the Network layer has no meaning to the lower layers. Therefore, before a packet is passed to the lower layers, a Network layer protocol like TCP/IP's Address Resolution Protocol (ARP) must resolve the logical address to the physical address usable by the Data Link layer.

Note

More about broadcasts: One important concept to understand is that networks at the Network layer represent broadcast domains. A broadcast is a packet that is sent to a special broadcast address. To understand what's special about it, consider that devices on a network in most cases receive every frame that crosses the network, but if the frame is not addressed to them specifically, they stop processing the packet or "drop" it. However, every device on a network will receive every broadcast and continue processing it by passing it up through the layers of the OSI model to the appropriate program. This behavior is necessary because there are many times when you need to send a message to every device on the network. It is not very scalable, because once you have more than a few thousand devices on a network, almost all the available bandwidth is used by broadcast packets, which leaves little to none for the all-important user data.

The solution to this problem was to limit the range of a broadcast to a local area, called a "broadcast domain." So when routers receive a broadcast from one network, they do not forward it to other networks. This is why we say that routers separate broadcast domains. Thus, one of the keys to designing high-performance enterprise networks is knowing how many broadcasts each device will send. This is based on the Network layer protocol you choose and calculating the optimal number of devices per network so that you minimize the number of networks you have to support without limiting the bandwidth.

An increase in traffic, including more and more streaming video, which loses its meaning if it does not arrive in the order in which it was sent, has inspired development and implementation of **Quality of Service (QoS)** standards. If QoS protocols and services have been implemented, they prioritize data in the Network layer. An example of QoS in action is the delaying of e-mail traffic in favor of time-critical audio or video data.

Separate from the logical address of the Network layer, a network device has a physical address, identified at the Data Link layer that uniquely identifies it. The best and most common example of a physical layer address is the Media Access Control (MAC) address of Ethernet Network Interface Cards (NICs). This number is a six-byte value stored in the read-only memory (ROM) on each network card. A portion of the number identifies the manufacturer and remains the same for all network devices from that manufacturer. The remainder of the number uniquely identifies the device.

The **Data Link layer** is responsible for taking the logical data from the upper layers and breaking it down into appropriately sized units, called **frames**. Some protocols at this layer will resend data for which an acknowledgment is not received.

The quintessential Data Link layer device is a **bridge**, which can be used to physically segment a network. It forwards or discards frames based on the physical address of the frame. If the destination **Media Access Control (MAC) address** is located on a segment other than the originating segment, it is forwarded. If the MAC address is on the local segment, the frame is discarded. What it cannot do is block MAC layer broadcasts the way a Network layer router can block broadcasts to logical addresses. When a bridge receives a frame with a MAC broadcast address, it forwards it. We will revisit the Data Link layer later in this chapter in a section on the IEEE standards.

Note

The MAC broadcast address is ff-ff-ff-ff-ff-ff. A Network layer address (logical address) may be shown as a broadcast to all subnets—255.255.255.255—or to just one subnet—131.107.255.255, which is a broadcast to the 131.107.0.0/16 subnet. There will be more on IP addressing in Chapter 4.

The **Physical layer**, at the bottom of the OSI reference model, encodes the transmission of the bits over the physical medium, whether electrical or optical. It also receives transmissions from the network. The Physical layer includes the media that carries the signals (copper wire, fiber-optic cable, or wireless) and physical devices for connection and control, such as NICs, repeaters, **hubs**, Multistation Access Units (MAUs), and **switches**. The Physical layer defines the physical **topology** of the media, and the protocols for translating signals appropriately onto and from the media.

Physical and Data Link Layer Standards and Technologies

Physical and Data Link layer standards define network topology, or the physical and logical layout of a network. This includes the transmission media, hardware, and related protocols used to connect network resources and also defines how computers are linked together.

The four common physical topologies are bus, star, ring, and mesh. After defining these topologies, we provide an IEEE 802 specifications review. These specifications pair up technologies from the Physical and Data Link layers of the OSI model into workable LAN and WAN solutions—the technologies underlying the Windows 2000 protocol and service infrastructures you will design. For infrastructure design, you also need to understand the concept of network backbone and the technologies used to implement them, discussed later in this chapter.

Bus Topology

The "classic" bus topology has computers strung out along a single cable, which must be terminated at each end so that the electrical signals transmitted on the wire do not reflect or bounce but instead get absorbed. If they do bounce, they can be sensed more than once by each device, which can cause data errors. Figure 1-4 illustrates the bus topology.

Years ago such a topology was practical for a very small network because it was inexpensive. The bus topology had several drawbacks though, including being difficult to troubleshoot, because a break anywhere in the cable would take down the entire network.

The most common LAN implementation, Ethernet, is built on the bus concept, and small Ethernet networks in the 1980s would use a physical bus. Essentially, on a bus topology network, the more traffic there is, the more collisions that will occur because of the access method.

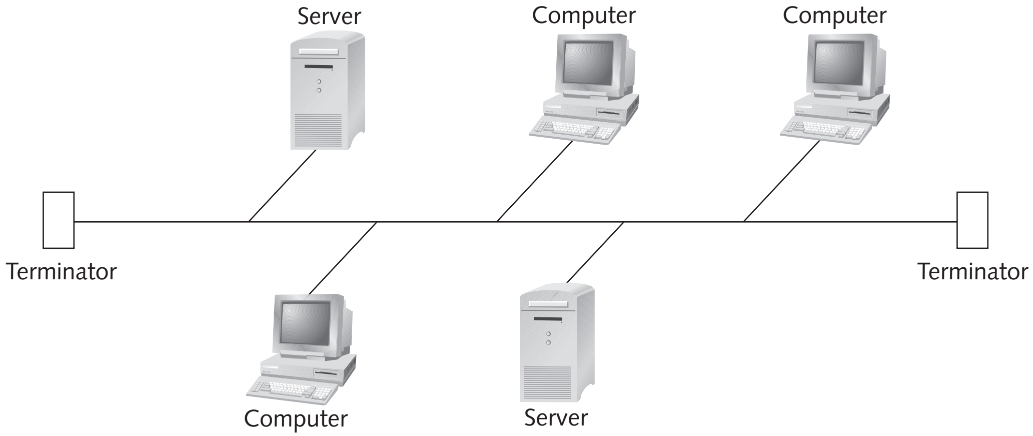

Figure 1-4 Bus topology

Star Topology

Each device in a star topology network is cabled directly to a central hub. The connection to a hub creates a physical star. There are two types of hubs. An active hub, also known as a multiport repeater, will actually regenerate the signal and send it on to all devices connected to the hub. A passive hub (a punch-down block or wiring panel) is simply a nonpowered connection point for organizing the cables. Star topology is more easily expanded than a bus topology; a computer can be added to or removed from the network without taking the entire network down. See the star topology illustrated in Figure 1-5.

The most common implementation of a star topology physically resembles a star but logically is a bus. This is an Ethernet network connected to a hub. The Ethernet bus is contained within an Ethernet hub, which manages the continuity of the bus, disabling a connection when a cable is disconnected or when the network card of the attached computer becomes disabled. Because of this, our bus-based Ethernet network is said to be logically using a bus topology, but physically using a star topology. For many years, Ethernet networks have most frequently been implemented with hubs instead of being connected directly to a single common cable.

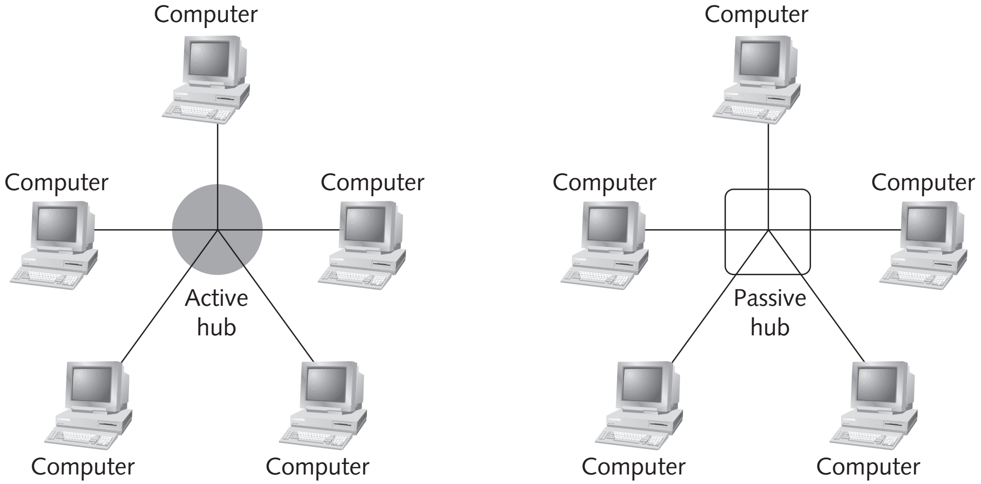

Figure 1-5 Star topology

Ring Topology

Each device in a ring topology is connected to the next device in the ring, and the last device is connected to the first. Each device regenerates and retransmits signals it receives to the next device in the ring in one direction. Ring networks tend to be more expensive than star networks because historically one vendor, IBM, has prevailed in this market, but they do not have the collision issues of bus or star topologies. Figure 1-6 illustrates the ring topology.

IBM's **Token Ring network** uses a special packet called a token to grant a given workstation access to the network. This avoids collisions altogether. Token Ring networks operate at speeds of 4 Mbps, 16 Mbps, and 100 Mbps.

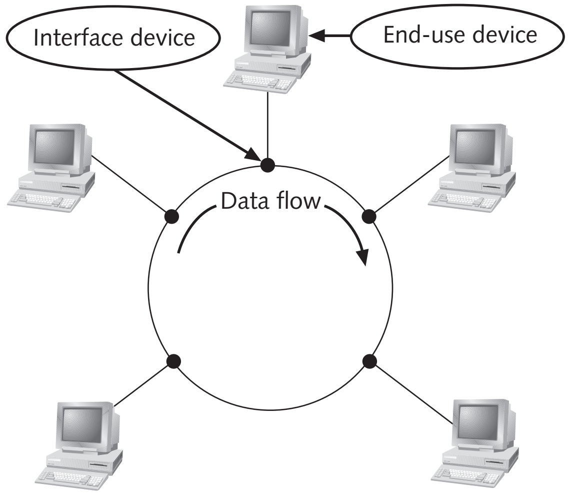

Figure 1-6 Ring topology

Mesh Topology

In a mesh topology network, there are redundant paths to each device on the network. A full mesh topology gives each network device a connection to every other network device. This is a very expensive design, but the high level of **redundancy** eliminates downtime if one device fails. The importance of redundancy becomes crystal clear when you consider how long a bank or a hospital could survive without their WAN links. Figure 1-7 illustrates the mesh topology.

An actual physical mesh is more theory than practice. You are only likely to find full mesh topology on a network backbone. In a hybrid mesh topology, only selected devices are given redundant links; others have only one connection to the network. This could describe routed networks, in which the routers have redundant connections to each other. Even in this example, the routers may not have full redundancy, meaning each router is not connected to each and every other router.

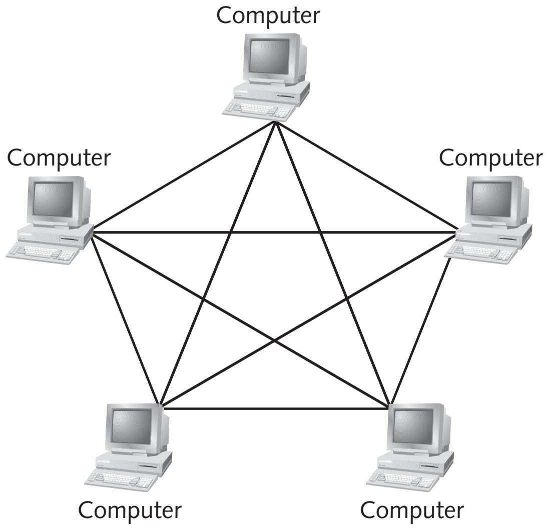

Figure 1-7 Mesh topology

Hybrid Topology

Most often, networks represent variations and hybridizations of the basic network topologies. Ethernet networks are derived from a bus model, but they are implemented as physical star networks with logical buses. The physical topology follows the media, while the logical topology follows the data.

Ethernet hubs and switches are at central points for connection of wires, but the data actually travel on a bus within these devices. Token Ring networks are star-wired with special hub-like devices, MAUs, but inside these devices the data flow on a ring. Each computer on the network becomes part of the ring when connected to the hub.

Organizations often have both of these, as well as other varied networks. Add the need to connect to mainframe and mini-computer systems, and you may well have a hybrid topology resembling Figure 1-8.

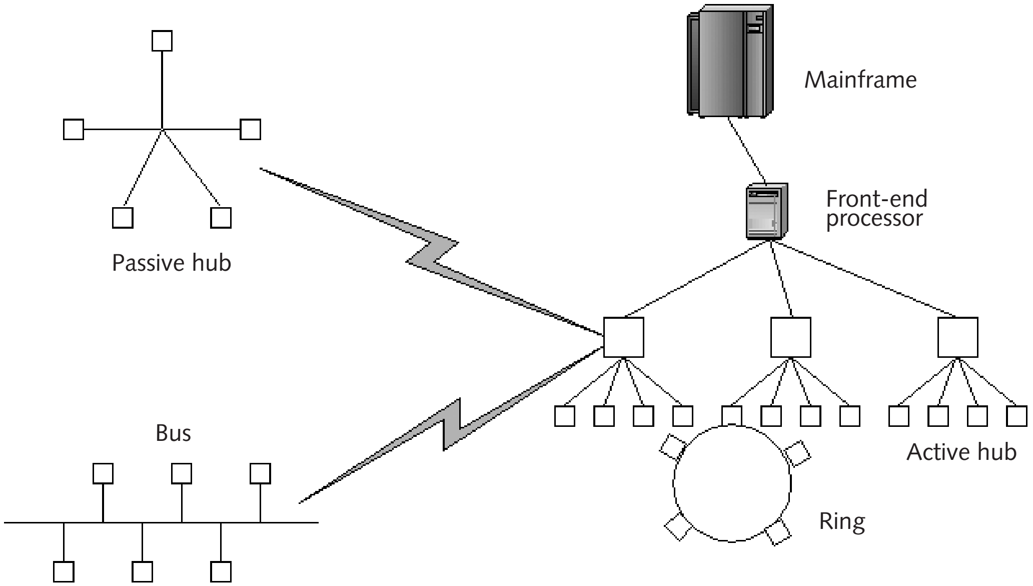

Figure 1-8 Hybrid topology

Switched Networks

With the dramatic increase in the use of Internet browsing, multimedia applications, graphic-intensive communications, and e-mail, the volume of network traffic in most organizations has expanded exponentially. Network managers are constantly faced with disappearing bandwidth. Rather than replace the entire existing network infrastructure, these managers look for solutions that integrate well with their existing networks and optimize what they already have. Switching hubs usually fit right into this strategy.

A switching hub (often known simply as a switch) is a device that replaces a hub. Rather than regenerate a frame on every port, which means every computer has to process it, a switch only sends the frame to the computer it is addressed to, effectively isolating the traffic so that the other devices connected through the switch do not sense it. Switches route the frames based on address, usually the physical address. Thus a 10 Mbps or 100 Mbps LAN now behaves as though it has many 10 Mbps or 100 Mbps segments operating within it, greatly increasing the effective bandwidth. Switches effectively create more bandwidth by segmenting the network at layer 2, giving each device its own dedicated segment and allowing devices to operate full duplex, sending and receiving at the same time. This means twice as much bandwidth and no contention on the wire (although there is now contention in the buffers and backplane of the switch).

Note

Layer 2 virtual LANs (VLANs), using physical ports, are not to be confused with the virtual private networks (VPNs) of layer 3 that use logical addresses.

IEEE 802 Specifications Review

In February 1980, the Institute of Electrical and Electronics Engineers (IEEE) met to develop standards for the Physical and Data Link layers of the OSI reference model. These standards include cabling, topologies, and media access methods. The standards that grew out of this and subsequent meetings of various committees of the IEEE all have the prefix 802, "80" representing 1980 and "2" representing the second month. The 802 is followed by a decimal point and the number of a section of the 802 project, as described in Table 1-1.

Table 1-1 IEEE 802.x specifications

IEEE Section	Description of Standard
802.1	Communications between WANs or LANs (as in 802.1d, the Spanning Tree Algorithm)
802.2	Logical Link Control (LLC) for 802.3, 802.4, 802.5, 802.6
802.3	Contention-based Ethernet
802.4	Bus topology token-passing
802.5	Star or ring topology token-passing
802.6	MAN distributed queue dual bus
802.7	Broadband network installation and maintenance
802.8	Fiber-optic
802.9	ISDN time-sensitive Ethernet voice and data communication
802.10	LAN security
802.11	Wireless LANs
802.12	Contention-based 100 Mbps networks

Among the most important works of the 802.x groups was the determination that the Data Link layer of the OSI reference model needed to be further subdivided into two layers: the **Logical Link Control (LLC)** portion at the top of the Data Link layer and the **Media Access Control (MAC)** portion beneath that. Figure 1-9 illustrates the mapping of the IEEE 802.x standards to the OSI reference model.

The LLC sublayer, as defined in IEEE 802.2, includes flow control and management of connection errors, while the MAC sublayer is defined in the 802.3, 802.4, 802.5, 802.6, 802.9, 802.11, and 802.12 standards. The MAC sublayer includes a physical address, often referred to as the MAC address, a unique address in ROM on every NIC. This address is represented as six bytes, typically displayed in hexadecimal, and can be viewed using utilities such as the IPCONFIG utility of the Windows 98 and NT TCP/IP stack or the WINIPCFG utility of Windows 95.

Note

Try Hands-on Project 1-5 to discover the physical address of a local network card and Hands-on Project 1-6 to discover the physical address of a remote computer.

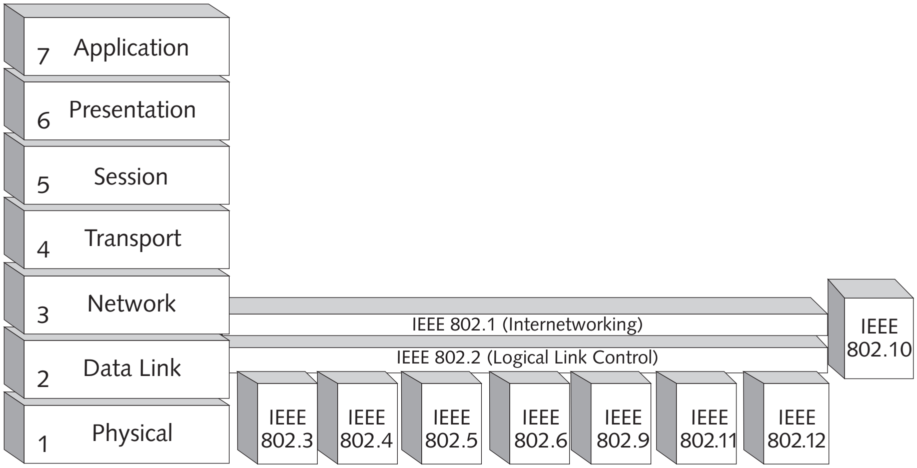

Figure 1-9 IEEE 802.x standards mapped to the OSI reference model

Ethernet

Ethernet is the most popular LAN specification used today. It started out as a network design developed in 1976 by Xerox Corporation in cooperation with DEC and Intel. Later, it was formally adopted by the IEEE as part of 802.3. Ethernet uses a bus or star topology physically, although it is always a bus logically. It includes protocols and standards for both the Physical and the entire Data Link layer of the OSI reference model.

The IEEE defined standards for Ethernet-type networks in the IEEE 802.3 standard, which includes specifications for the OSI Physical and MAC layers. The IEEE 802.2 standard defines the Logical Link Control sublayer functionality of Ethernet and other network types.

Ethernet uses a **baseband** signal over a logical bus topology, implemented on a physical bus or star topology. Baseband means that the medium can only carry one signal or channel at a time. Ethernet can use several physical media types, including coaxial, twisted-pair, and fiber-optic. Today, Ethernet networks operate at speeds of 10 Mbps, 100 Mbps, and 1,000 Mbps (Gigabit Ethernet).

802.3 includes the following specifications:

- *10Base2:* Commonly known as "thinnet" because it uses a thin coaxial cable
- *10Base5:* Commonly known as "thicknet" because it uses a thick coaxial cable

- *10BaseT:* Runs over twisted-pair copper cable
- *100BaseTx:* Commonly known as "Fast Ethernet"
- *100BaseFx:* Runs over fiber-optic cable

There are new specifications for Gigabit Ethernet as well. 802.3z defines 1000BaseSx and 1000BaseLx as standard for Ethernet over fiber. For copper, the 802.3ab standard describes the specifications for 1000BaseT twisted-pair Gigabit Ethernet.

Tip

For more information about Gigabit Ethernet, visit www.gigabit-ethernet.org.

Ethernet uses the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) media access method to handle simultaneous network access demands.With this access method, a node (or device) wanting to transmit on the network listens for traffic (carrier sense). If no traffic is detected, the node sends a carrier signal. Other nodes wanting to place frames on the line sense the carrier and go into a "defer" mode, because only one node is permitted to transmit at a time.

However, more than one node may simultaneously sense that there is no carrier on the media and attempt to transmit. The resulting collision is detected by the transmitting nodes (collision detect). Once a transmitting node detects a collision, it sends a special "jam" signal to notify all listening nodes that a collision occurred. Each node then uses an algorithm to determine the amount of time it will wait before retransmitting. The "multiple access" designation of CSMA/CD refers to the ability of an Ethernet device to place multiple frames on the media in succession (as opposed to Token Ring, where you send a frame and then hand the token to the next guy).

Token Ring

The second most popular LAN technology in use today was developed in the 1970s by IBM. A Token Ring network has a physical star topology but a logical ring topology. All the computers in a Token Ring network are connected to one or more MAUs, a Token Ring hub that maintains the ring.

IBM's Token Ring maps to both the Physical and Data Link layers of the OSI reference model. As with Ethernet, the IEEE addressed this existing technology in its 802 standards, defining just the Token Ring MAC sublayer and Physical layer protocols in 802.5, and including LLC sublayer protocols of Token Ring and other network types in 802.2.

Fiber Distributed Data Interface

The American National Standards Institute (ANSI) X3T9.5 standards committee created the Fiber Distributed Data Interface (FDDI) standard in the 1980s for high-speed 100 Mbps data communications over fiber-optic cable spanning distances up to 200 kilometers. FDDI maps to the Physical layer and the MAC sublayer of the Data Link layer of the OSI reference model, as shown in Figure 1-10.

FDDI uses a timed token access method for network communications. This method allows multiple frames from several different nodes to be on the network simultaneously. The FDDI standard allows for priority levels for hosts or data types, and can handle both **synchronous** packets, for time-sensitive communications, and **asynchronous** packets, for other traffic. Because it is time sensitive, synchronous communication is used for voice, video, and multimedia communications that must be sent in a nonbroken stream. For fault tolerance a FDDI network actually has two rings, primary and secondary. FDDI hubs and other network equipment are designated as Class A devices and, as such, attach to both rings.

In a FDDI network, servers and client computers are Class B devices that gain access to the FDDI network through Class A devices, which are able to detect failure of a ring and reconfigure the architecture to use a single ring. If the secondary ring is not being used as a backup, but instead is carrying traffic, the effective transmission rate can increase to 200 Mbps.

There are existing FDDI installations, especially in backbone networks, but 100 Mbps Ethernet on fiber-optic cabling is used more often, because it is scalable and easier to manage than FDDI.

Note

Backbones are usually populated with servers, while client computers reside on Ethernet or Token Ring networks bridged to the backbone. FDDI is defined in IEEE 802.8. Read more about backbones in the "Network Backbones" section of this chapter.

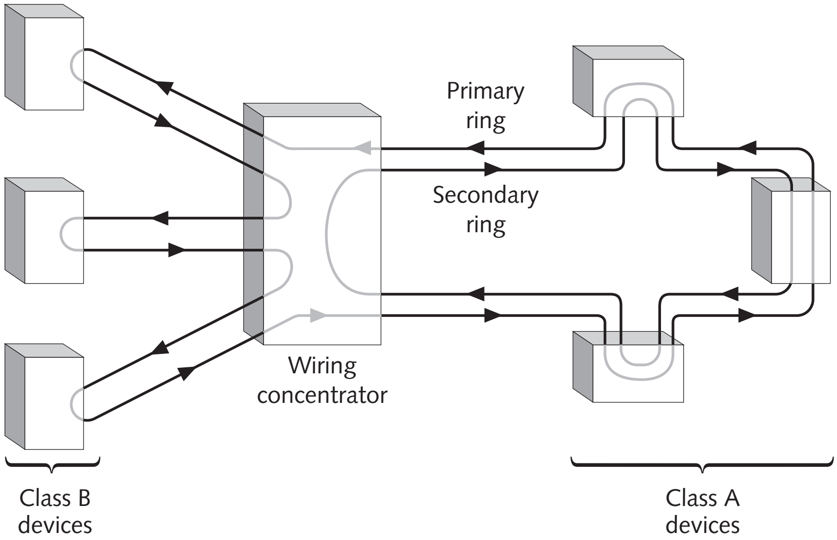

Figure 1-10 FDDI topology

X.25

The International Telegraph and Telephone Consultative Committee (CCITT) developed the X.25 **packet-switching** network specification in 1974 for WAN connectivity. On its own, X.25 maps to the Network layer of the OSI reference model, but it is normally used over Link Access Procedures-Balanced (LAPB), a Data Link layer protocol. LAPB runs over a CCITT Physical layer protocol, such as X.21, X.21bis, or V.32. Figure 1-11 illustrates the X.25 mapping to the OSI reference model.

X.25 is commonly used for international communications, because most countries have X.25 networks available through their telephone systems. X.25 provides reliable communications and end-to-end flow control over permanent or switched virtual circuits. In spite of recent improvements in speed, however, X.25 has a low relative throughput because so much bandwidth is used for error checking. For this reason, when there is a choice, Frame Relay is chosen over X.25.

Frame Relay

Frame Relay is a packet-switching standard defined in CCITT recommendations I.451/Q.931 and Q.922. It maps to the Physical and Data Link layers of the OSI reference model. Like X.25, it uses virtual circuits for WAN connectivity; unlike X.25, it leaves most error-checking and monitoring tasks to upper-level protocols, which contributes to its speed of 56 Kbps to over 45 Mbps (depending on the physical transmission media). Figure 1-11 also shows the mapping of Frame Relay to the OSI reference model.

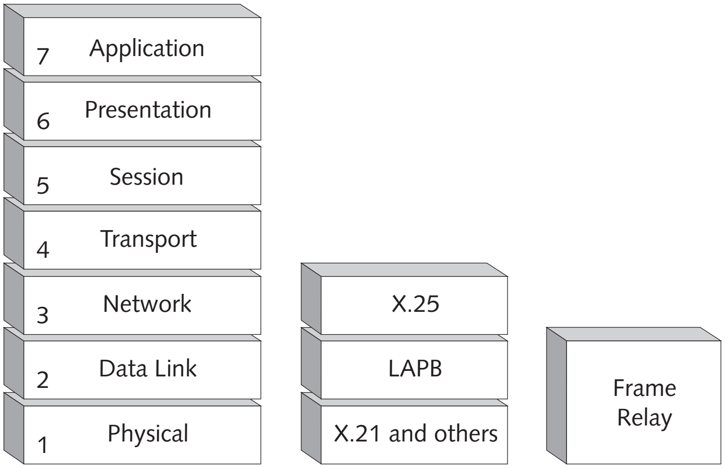

Figure 1-11 X.25 and Frame Relay mapped to the OSI reference model

Note

The CCITT has since been renamed the International Telecommunications Union (ITU).

Frame Relay is newer than X.25 and is a popular choice for connecting **remote offices**. Using permanent virtual circuits (PVCs), it creates pathways through the packet-switched network of the provider. Switched virtual circuits (SVCs) are also available. These allow communications without predefined circuits. In addition to the purchased Frame Relay service, the customer also needs a dedicated connection to the Frame Relay provider. This connection must match the speed of the Frame Relay service.

When connecting remote sites separated by great distances, Frame Relay networks are less expensive than leased lines because you only need to lease circuits to the Frame Relay provider's nearest point of presence (POP). You also have more flexibility with Frame Relay, because when you arrange for Frame Relay service, you specify several requirements for the bandwidth to be used. This includes a minimal amount of bandwidth that will be provided. The name for this baseline is the Committed Information Rate (CIR). If you believe you will need to exceed this bandwidth, you may specify a higher burst rate, which is the maximum amount of bandwidth that the Frame Relay provider will allow.

Tip

For more information about Frame Relay, go to www.frforum.com.

Integrated Services Digital Network

An **integrated services digital network (ISDN)** is a CCITT transmission media standard for telecommunications that includes the capability to transmit voice, data, and video signals over the same media—a digital telephone network. A variation on ISDN, broadband ISDN (B-ISDN), provides more bandwidth and can be used over SONET and ATM (defined below). ISDN maps roughly to the OSI Physical layer through the Network layer, but is often implemented as a fancy Data Link protocol over which we transport IP traffic. Figure 1-12 illustrates the mapping of ISDN to the OSI reference model.

It employs time-division multiplexing (TDM) at the Physical layer and the Network layer functions defined by CCITT recommendations I.450/Q.930 and I.451/Q.931. Another protocol, Link Access Procedure D Channel (LAPD), provides the Data Link layer functions for acknowledged, connectionless, **full-duplex** communications. LAPD provides physical device addressing at the MAC sublayer and flow control and frame sequencing at the LLC sublayer.

Tip

To learn more about ISDN standards, go to:
www.ralphb.net.

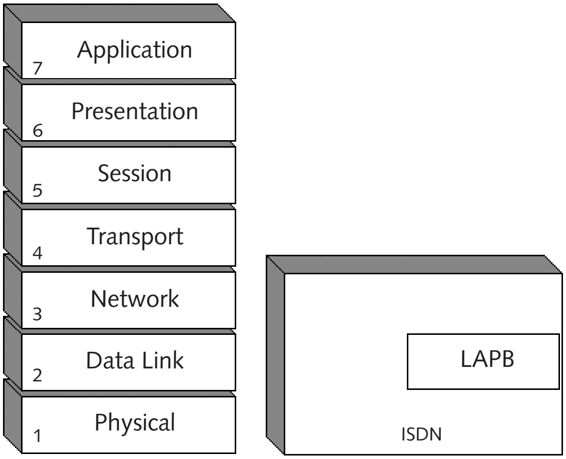

Figure 1-12 ISDN mapped to the OSI reference model

In ISDN, one channel, the D channel, is used for control, and separate channels, B channels, are for data. B channels are always bi-directional 64 kbps; D channels vary in size.

When you purchase ISDN service, you have two major choices: basic rate interface (BRI) and primary rate interface (PRI). BRI, which is sometimes called 2B+D, is two 64 Kbps B channels and a single 16 Kbps D channel over a single 192 Kbps circuit. If you are doing the math, you will notice some unaccountable bandwidth. This is used for framing. BRI can simultaneously support two calls over the two B channels. PRI is the service intended for an ISP needing to multiplex many calls. It is sometimes called 23B+D because it provides 23 64 Kbps B channels and a single 64 Kbps D channel, an entire T-1 carrier.

Synchronous Optical Network/Synchronous Digital Hierarchy

Synchronous Optical Network (SONET) is a high-speed Physical layer protocol standard for WAN technology using fiber-optic cable. Bell Communications Research developed SONET. A similar standard, Synchronous Digital Hierarchy (SDH), was developed by the International Telecommunications Union (ITU). Variations of these standards allow for regional differences in telecommunications, such as SDH-Europe, SDH-SONET (North America), and SDH-Japan. These standards allow for **point-to-point** connections over mesh or ring physical topologies and use the **time-division multiple access (TDMA)** multiplexing method. See the illustration of SONET/SDH mapped to the OSI reference model in Figure 1-13.

Asynchronous Transfer Mode

The ITU Telecommunications Standards Sector and the ATM Forum are working together on the **Asynchronous Transfer Mode (ATM)** standard, used mainly in WANs, but also in LANs and MANs. ATM provides both dynamic (through SVCs) and static (through PVCs) route selection and uses cell switching, where a cell is defined as a fixed-length 53-byte packet that follows a virtual circuit. This is what distinguishes ATM from Frame Relay and X.25. The latter two technologies switch packets, which can be variable in length and, therefore, require overhead to define and manage.

This fixed cell length also makes ATM data transfer rates more predictable and reduces both latency and jitter. For these reasons, ATM's LAN support, local area network emulation (LANE), is used for high-speed, multimedia networking across the enterprise network.

ATM runs at speeds of up to 155 Mbps, 622 Mbps, 2.4 Gbps, and even 10 Gbps. This last one is often cryptically referred to as OC-192. This refers to SONET Optical Carrier levels, which also maps level-to-level with the SDH international standards. These are defined as a standard rate of transmission of 51.84 Mbps, called a Synchronous Transport Signal level 1 (STS-1), as shown in Table 1-2.

Table 1-2 Synchronous Transport Signal and Optical Carrier Speeds

Synchronous Transport Signal Rate	Optical Carrier Level	Speed
STS-1	OC-1	51.84 Mbps
STS-3	OC-3	155.52 Mbps
STS-12	OC-12	622.08 Mbps
STS-24	OC-24	1.244 Gbps
STS-48	OC-48	2.488 Gbps
STS-96	OC-96	4.976 Gbps
STS-192	OC-192	9.952 Gbps

Mapping to the OSI Network and Data Link layers, ATM can run over FDDI and SONET/SDH Physical layer protocols, but most often is run over FDDI. ATM can even be deployed over existing category 5 cabling. Figure 1-13 shows ATM mapped to the OSI reference model.

As a connection-oriented technology, ATM requires a discrete path between two network endpoints before data can be exchanged. There is more setup time for network managers, because each of these connections must be preconfigured through an ATM dynamic routing protocol, such as Private Network-to-Network Interface (PNNI), which distributes topology information to each switch on the network. The switches, in turn, calculate the best path between endpoints. If there are link failures, the PNNI protocol responds by calculating alternate paths.

Unlike connectionless LAN technologies, such as Ethernet and Token Ring, in which the amount of bandwidth available to each client decreases as you add nodes to the network, in an ATM network, bandwidth can be dedicated to each device. For example, you can allocate 25.6 Mbps to a desktop application and full 155 Mbps to an application server. This allocation of bandwidth is a function of the service class and corresponding QoS setting. In spite of these features, ATM is not widely used because it is expensive and because of the increased development of fast Ethernet standards.

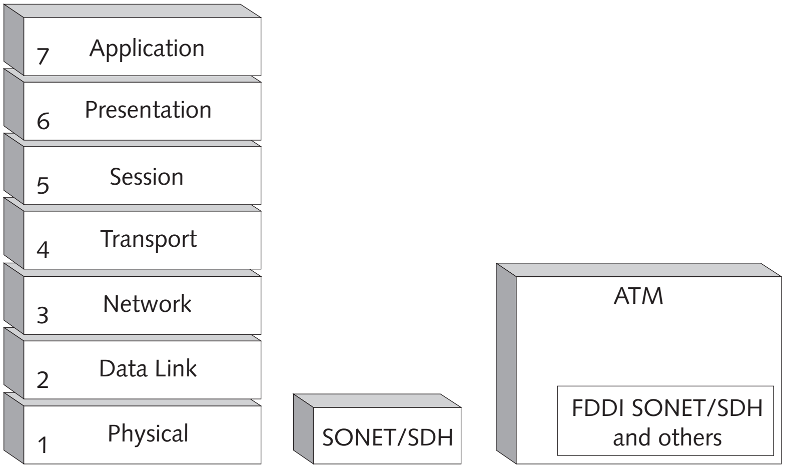

Figure 1-13 SONET/SDH and ATM mapped to the OSI reference model

Tip: For more information about ATM, go to www.atmforum.com.

Switched Megabit Data Service

Bell Communications Research developed Switched Megabit Data Service (SMDS), a cell-switching technology with **isochronous** (time-dependent) transmission synchronization. SMDS maps to the Data Link and Network layers of the OSI reference model and can be run over SONET/SDH. Figure 1-14 illustrates the mapping of SMDS to the OSI reference model.

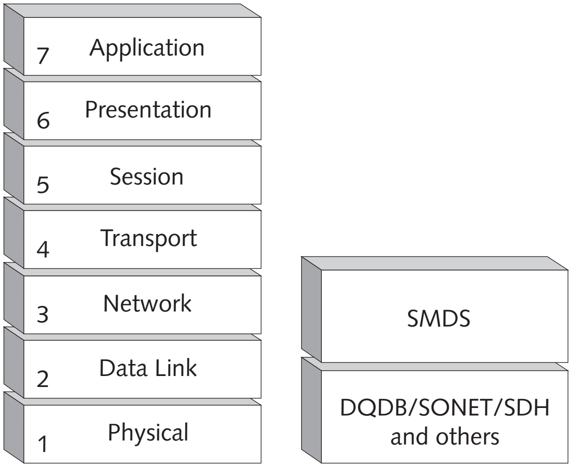

Figure 1-14 SMDS mapped to the OSI reference model

T-Carrier System

Bell Telephone Laboratories developed the **T-carrier system** in the 1960s for multiplexing voice signals onto digital transmission lines. The T circuits are digital, full-duplex transmission systems operating at 64 Kilobits per second per channel. The individual channels can be configured for either voice or data. The levels of service available are T-1, fractional T-1, and T-3.

T-1 consists of 24 individual channels that, transmitting 64 Kbps each, deliver a total throughput of 1.544 Mbps. Fractional T-1 is one or more of the individual T-1 channels that can be leased from a telephone company as a cheaper alternative to an entire T-1 line.

A T-3 line consists of a dedicated phone connection consisting of 672 individual channels, each of which supports 64 Kbps. In total, a T-3 line supports data rates of about 43 Mbps.

Network Backbones

A backbone is a physical segment of a network used as a common connection point for other network segments. It is more often one or more actual physical segments. In addition to being central to the network, many servers are connected directly to the backbone to afford the best **availability**, reliably providing support services when needed.

End-user computers are not directly connected to the backbone. Because the backbone essentially **aggregates** traffic, it needs to be capable of carrying a greater load than other segments. Therefore, it is usually configured with a faster network solution at the Physical and Data Link layers than the configuration used on the end-user-populated segments. A layer 2 backbone could be a switch that connects all the other switches and hubs. A layer 3 backbone example would be the Network Service Providers (NSPs) on the Internet.

Some network backbones simply run 100 Mbps Ethernet or FDDI. However, when the user segments are also running at these speeds, a faster technology is needed for the backbone. For this reason, more and more network managers are moving to 1,000 Mbps Ethernet or newer ATM technologies for the backbone.

Network Connectivity Models

Most organizations will have a network with multiple characteristics, including combinations of the following elements:

- Many LANs connected by routers
- A high-speed backbone
- More than one network protocol stack in use, such as TCP/IP or IPX/SPX

- Dial-up connectivity to give remote users access to network resources
- Connections to external networks
- Demand-dial or dedicated connections between the main network and branch offices

We organize these elements into several basic network connectivity models that are used throughout this book. We look first at designing for these structures individually, then combining them into a comprehensive infrastructure design. These network connectivity structures are:

- Intranet
- Remote access
- Remote office
- Internet
- Extranet

For the most part, the TCP/IP suite of protocols (the Windows 2000 default network protocol suite) provides the layer 3 through 7 protocols and services, but in a later chapter, we look at integrating other networking protocols into our network designs.

Intranet

An **intranet** is a private network (LAN) providing the traditional services of file and print sharing, client/server applications, and software distribution, but also employing Internet-type services, such as e-mail, **newsgroups**, web sites, **web browsers**, and **File Transfer Protocol (FTP)** sites. Figure 1-15 illustrates an Intranet network model. Although an intranet uses Internet technologies, the information is usually intended for the internal audience.

Note

E-mail is electronic mail; a newsgroup is an Internet application that allows users to read and post articles on a hosting news server; a web browser is the client software for accessing Internet web servers; FTP client software allows you to transfer files between your computer and a specialized FTP server.

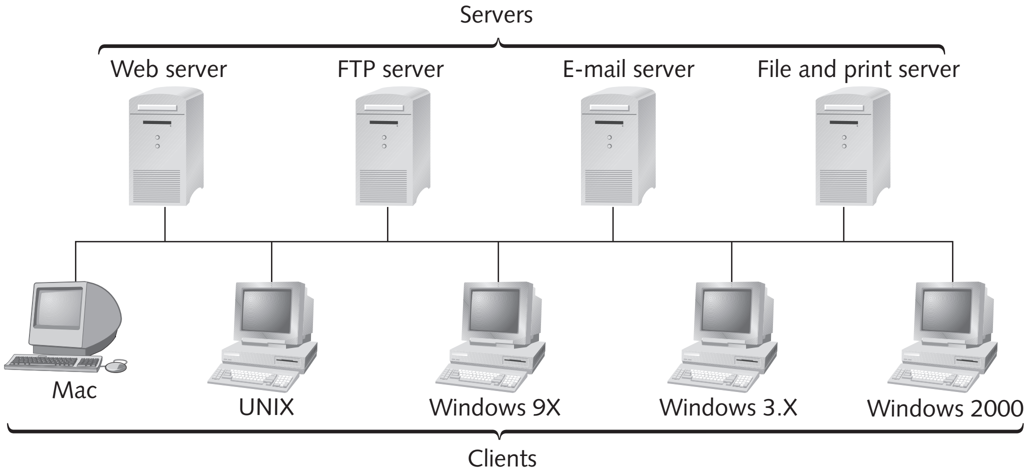

Figure 1-15 Intranet network model

Remote Access

The **remote access** connectivity model provides all the normal LAN services to users who telecommute, **mobile workers**, and technical support people who manage servers at remote locations. Figure 1-16 shows an example of the remote access model. The two main methods of remote access are direct dial and virtual private network. These connections are usually temporary and initiated by the remote worker.

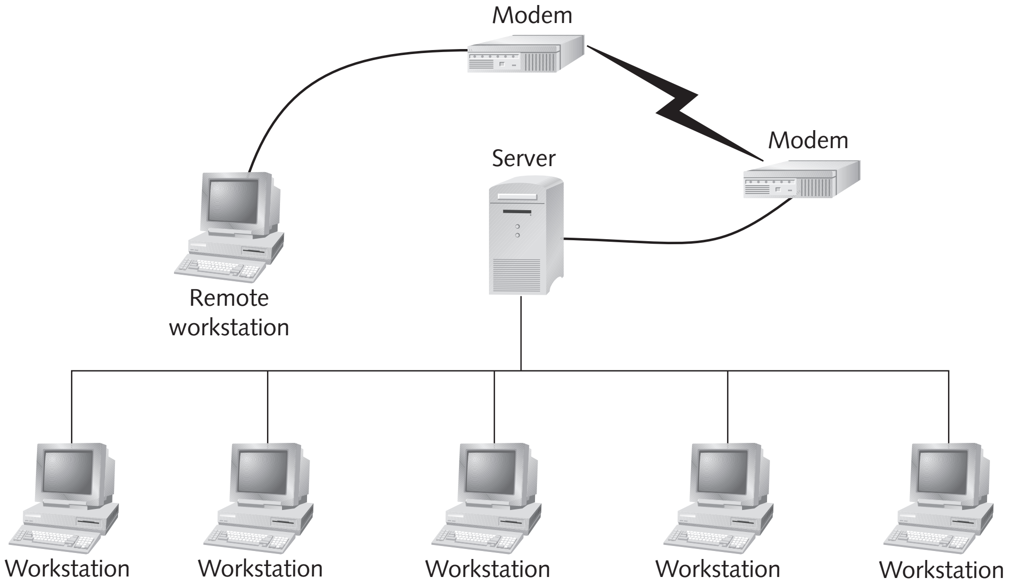

Figure 1-16 Remote access model

Direct Dial

Direct-dial remote clients use the public telephone network via modem or ISDN to connect to a server on a private intranet. The server then can either act as a gateway to the rest of the network or restrict the users' access to just that server. Direct dial may be an appropriate remote access solution if there are very few remote users or they are all within the local calling area.

Virtual Private Network

More secure remote access can be achieved using a **virtual private network (VPN)** over the Internet, in which case the client first completes a connection to the Internet, then establishes a VPN, over the Internet connection. The server on the private network to which the client connects can then act as a gateway to the network resources. Not only does this give a secure connection over the public Internet, but users outside the local calling area are able to connect toll-free.

Remote Office

In the remote office connectivity model, as illustrated in Figure 1-17, the LANs of one or more offices are connected to a central corporate LAN through persistent WAN links, as opposed to the usually temporary connections made for individual remote users. These LAN-to-LAN connections make up a corporate WAN, connected by routers.

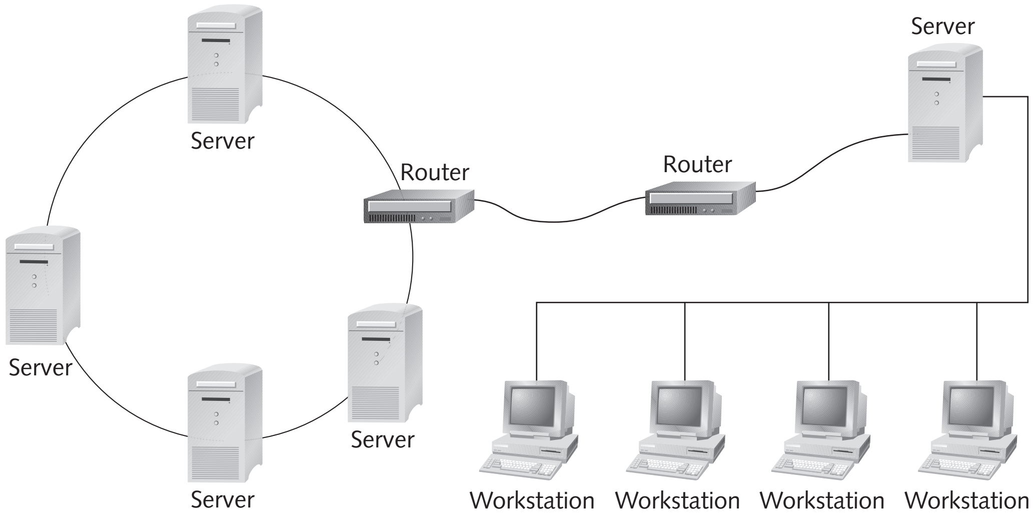

Figure 1-17 Remote office model

Internet

The Internet is the worldwide—and world-famous—mother of all TCP/IP networks. It is actually a collection of networks hosting a huge variety of services and products for individuals and organizations. More and more workers want or require reliable access to the Internet in order to accomplish their work. Therefore, network designs must take into consideration how to provide this access, as shown in Figure 1-18. Internet access is usually provided through either a dial-up or a dedicated line to an Internet Service Provider (ISP).

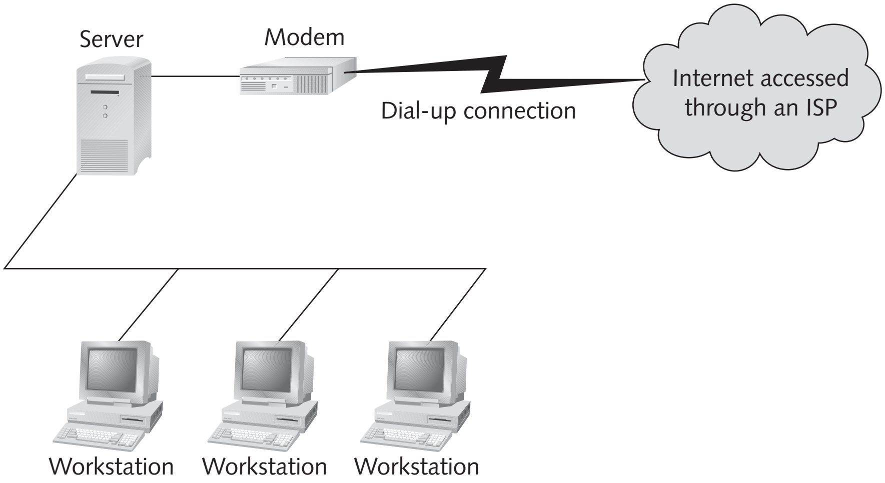

Figure 1-18 Internet model

Dial-up

Dial-up is the best solution for the SOHO crowd (Small Office/Home Office). Until a few years ago, the only option for most people was a modem connection. Now, depending on the local service, many individuals have access to ISDN, cable modem, or one of the various digital subscriber line (DSL) options for connecting to their ISP.

Dedicated Line

When many users on an intranet need Internet connectivity, one solution is a dedicated T-carrier connection. There are many other solutions, including ISDN PRI, SONET, or ATM. Some providers are offering Gigabit Ethernet Internet connections. Analysis of the actual bandwidth requirements will determine the level of service needed.

If you are considering a T-carrier, the choices are fractional T-1, T-1, and T-3 with speeds from 64 Kbps to 43 Mbps.

Extranet

An **extranet** includes LANs or intranets owned by separate organizations, which want their networks to be connected to accomplish one or more business objectives. An extranet could consist of a supplier and its customers. It is likely to use Internet technologies, such as e-mail and web server, and may reveal only a portion of a company's intranet to the collaborative partner, all of the network, or a separate network that is only shared between the partners. The typical extranet connection is through a secure VPN. Figure 1-19 illustrates one example of an extranet.

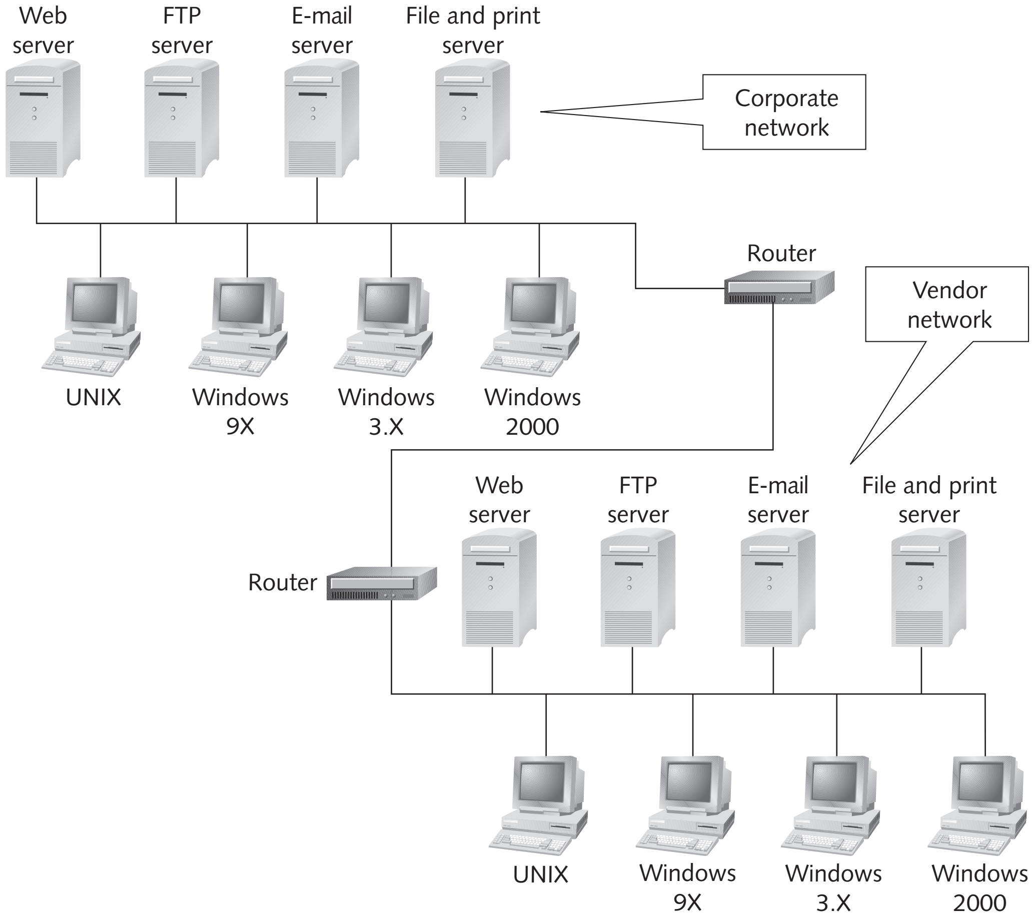

Figure 1-19 Extranet model

Windows 2000 TCP/IP Protocol and Services

This section is an overview of the protocols and services of the Windows 2000 TCP/IP suite. Most of the protocols and services are described here; some will be described in detail in subsequent chapters. There is a brief discussion of TCP/IP and the OSI model, as well as the more venerable Department of Defense (DoD) model.

TCP/IP Defined

TCP/IP is the protocol suite of the Internet and has become a standard for routed networks worldwide. It is also the network protocol suite that is installed by default by Windows 2000. TCP/IP design was originally based on a different network reference model, the four-layered **DoD model**, which existed before the OSI model. Generally speaking, nobody uses the DoD model anymore, but it deserves at least some mention here. When talking about TCP/IP protocols, it is common for network professionals to use the OSI terms. Figure 1-20 maps TCP/IP to the OSI reference model.

The top layer in the DoD reference model, Process/Application, maps to the top three layers of the OSI reference model, Application, Presentation, and Session. The second layer is Host-to-Host, which maps to the Transport layer of the OSI reference model. Further down, the Internet layer maps to the Network layer, and at the bottom of the model the Network Access or Network Interface layer maps to the Data Link and Physical layers of the OSI reference model.

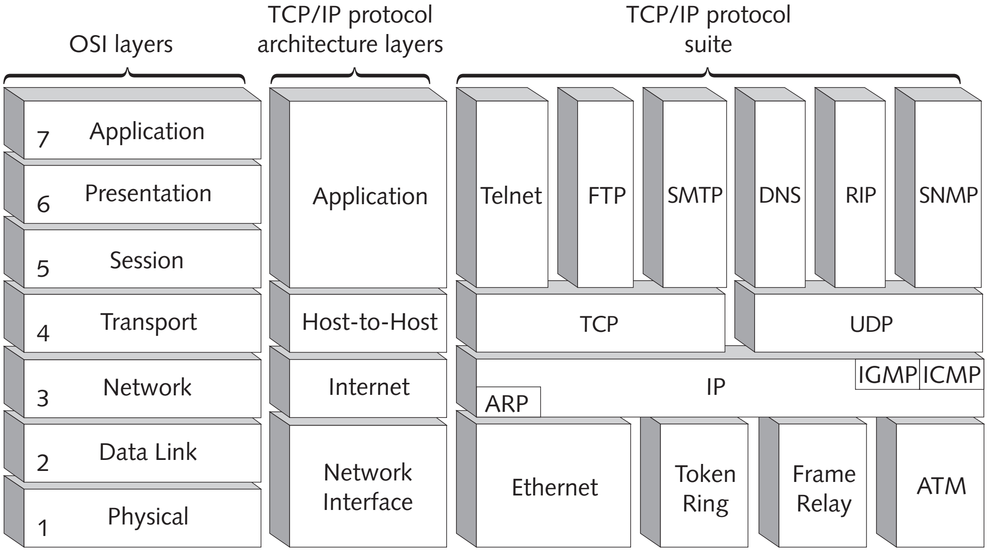

Figure 1-20 TCP/IP mapped to the OSI reference model

TCP/IP standards are the responsibility of the Internet Engineering Task Force (IETF), a subgroup of the Internet Society (ISOC), an organization of Internet experts that oversees a number of other boards and task forces dealing with network policy issues. Among the other subgroups of ISOC are the Internet Engineering Steering Group (IESG), the Internet Architecture Board (IAB), and the Internet Assigned Numbers Authority (IANA).

The IETF is concerned with developing protocol standards and is managed by the IESG. Standards are proposed and developed through a process of publicly posting documents for review and comment of people who choose to participate in the committees and task force. The proposed and accepted standards are published as Request for Comment (RFC) documents and can be viewed at www.ietf.org, which contains an index of RFCs by number. If you have not memorized these numbers (very likely) or do not know the RFC number for the standard you are researching, you will be happy to know that the IETF site includes links to other sites where you may search RFCs by number, author, title, date, and keyword.

What is truly remarkable about all this is that the Internet standards are voluntary. Most hardware vendors and software developers work to provide value in their products while following the Internet standards for the sake of continued interoperability of networks. Windows 2000 was many months in development, but Microsoft wanted to meet their design goals using the latest technology. For this reason, many of the protocols and services supported in Windows 2000 were based on proposed standards. As the release date neared, more and more of these achieved standard status. Rather than list each RFC as we discuss the individual protocols and servers, we have included an Appendix A of RFC's that currently apply to Windows 2000.

A TCP/IP network has three fundamental traffic types: **unicast**, broadcast, and **multicast**. Unicast traffic is sent to a unique address; broadcast traffic is sent to all devices; multicast traffic is sent to all addresses within a multicast group. There is much more to say about each traffic type. Some of this is revealed in the description of protocols and services in this chapter. More will come as we look at designing with the various protocols and services later in this book.

TCP/IP Application Layer Protocols and Services

Protocols at this level are involved in the application-to-application interaction that occurs between connected systems. Many of the applications that run over TCP/IP networks are client/server applications, in which a main component, the server, runs on one machine, responding to and providing services to the secondary component, the client, running on, well, the client computer.

Application layer protocols and services are not these actual programs, but give support to these programs. E-mail programs are a great example of this. Many people use Microsoft Outlook (the client) to access and manage messages on Microsoft Exchange (the server). Outlook makes requests of the Exchange server through Application layer components.

Telnet

The Telnet utility provides remote terminal emulation. A client computer using it can access host-based applications without concern for the local operating system. As a top-layer protocol, Telnet performs dialog control, session administration, connection establishment and release, and file transfer. It also provides the translation function and support to give users access to the network. Router administrators use the Telnet utility to connect to and configure routers.

File Transfer Protocol

With the use of the File Transfer Protocol (FTP), file transfer can take place between computers with dissimilar operating systems. FTP is both a service and a utility that will allow for **security** through a user name and password, and utilizes the host-to-host Transmission Control Protocol (TCP). The FTP utility, when executed, runs as a character-mode, or shell, application. As with many shell utilities in Windows, FTP can be used interactively or it can be automated through a script. FTP servers can also be accessed from an Internet browser that provides the FTP client in a graphical user interface (GUI). FTP is widely used on the Internet for downloading files.

Trivial File Transfer Protocol

The Trivial File Transfer Protocol (TFTP) allows for the transfer of files using the host-to-host User Datagram Protocol (UDP), which is less reliable than TCP. Because it also has no user authentication method, it is less secure than FTP. It only allows for transfer of files in one direction. Because of the lack of security in TFTP, Windows 2000 only includes the client side of TFTP, except in the special cases of Remote Installation Services and BOOTP. The Remote Installation Server (RIS) service uses TFTP to download the initial files needed to begin an installation. Similarly, when BOOTP is implemented in a Windows 2000 DHCP server, the BOOTP client uses TFTP to perform file transfer of the boot image.

Simple Mail Transfer Protocol

The Simple Mail Transfer Protocol (SMTP) is used on the Internet to transfer mail between mail servers. Clients also use this protocol to send mail to servers. When configuring a computer to access Internet e-mail, you will need the address or Fully Qualified Domain Name (FQDN) of an SMTP server to which your mail client will send mail. You will also need the address of a **Post Office Protocol (POP)** server from which your mail client will pick up mail.

Note

Most e-mail applications use POP, which has two versions. The first, called POP2, became a standard in the mid-1980s and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is a standard for network management used on both TCP/IP and Internet Package Exchange (IPX) networks. An SNMP management program, often called an SNMP console, would depend on this protocol to carry management information and commands to a network management agent running on a network device, such as a computer or router.

The agent on the device responds to the commands or preconfigured events by sending status information to the computers hosting the management consoles. The agent provides the information in a standard format, defined as Management Information Base (MIB). The Windows 2000 implementation of SNMP supports several versions of MIB, including the Internet MIB II, LAN Manager MIB II, Host Resources MIB, and the Microsoft proprietary MIB. Microsoft does not provide an SNMP console, preferring the newer, richer Web-based Enterprise Management (WBEM) standard. The Microsoft implementation of WBEM is Windows Management Instrumentation (WMI), also referred to as Windows Management. The Microsoft Management Console is the administrative interface for Windows Management.

The Microsoft TCP/IP includes an SNMP agent that will respond to the commands from a third-party management console. In addition, there is a sample SNMP manager program, SNMPutil.exe, in the Support folder on the Windows 2000 CD-ROM, intended to serve as an example of an application built on top of the Windows 2000 Management API.

Note

For more information on the Microsoft implementation of WBEM, Windows Management, search Windows 2000 help using the keyword "WBEM" or "Windows Management." Also, check out the source of the WBEM standard, the Distributed Management Task Force Inc. (DMTF), at www.dmtf.org/wbem.

Hypertext Transfer Protocol

The Hypertext Transfer Protocol (HTTP) is the information formatting and transfer protocol of the World Wide Web (WWW). Included in HTTP are the commands used by web browsers and web servers. The browsers, using HTTP, request web pages from web servers and then display them on the screen.

Dynamic Host Configuration Protocol Service

The Dynamic Host Configuration Protocol (DHCP) service can be installed on a computer running a Windows 2000 server product. Then, once properly configured, the DHCP service provides a system for the automatic issuance and management of IP addresses and other TCP/IP configuration parameters to client TCP/IP computers configured to be DHCP clients.

Domain Name Service

The Domain Name Service (DNS) can be installed on a computer running a Windows 2000 server product. Once configured appropriately, it can be used to maintain and manage a database of the domain tree structure and network service locations. DNS clients, known as **resolvers**, query DNS servers for name-to-IP-address resolution.

Windows Internet Name Service

The Windows Internet Name Service (WINS) can be installed on a computer running a Windows 2000 server product. A WINS server maintains a dynamic database of NetBIOS-computer-name to IP-address mappings. Computers configured as WINS clients register their names and services with the WINS server at startup. WINS clients also query WINS servers for NetBIOS name resolution.

Common Internet File System

The Common Internet File System (CIFS) is the newest incarnation of Server Message Block (SMB), the Microsoft file- and printer-sharing protocol. It includes both a protocol and a corresponding API to be used by application programs requesting access to network resources.

Internet Printing Protocol

The Internet Printing Protocol (IPP) allows users to print directly to a printer via its Universal Resource Locator (URL). This printer could be located on the Internet or on a corporate intranet. IPP uses the HTTP to send print jobs. Also, Windows 2000 automatically generates print-job information in HTML format, easily viewed in a browser. This means that clients do not have to be Microsoft file- and printer-sharing clients to be able to use a printer shared on a Windows 2000 server.

Network News Transfer Protocol

The Network News Transfer Protocol (NNTP) is used in the distribution of news messages between NNTP servers and NNTP clients (news readers such as Outlook Express). The NNTP server maintains a central store of new messages that can be retrieved by NNTP clients. Windows 2000 includes an NNTP service, which is used by Microsoft Exchange Server 2000. The NNTP service is configured through the latest version of the Microsoft electronic messaging server, **Exchange 2000**, for the purpose of hosting news groups.

Transport Layer Protocols

The Transport layer protocols define the level of transmission service, as in reliable end-to-end communications, versus unreliable broadcast communications. Protocols at this layer are also responsible for packet sequencing and data integrity. Host-to-host protocols include the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

Transmission Control Protocol

The Transmission Control Protocol (TCP) is a Transport layer protocol that enables guaranteed packet delivery over Internet Protocol (IP). To provide guaranteed delivery, TCP establishes end-to-end communications, a virtual circuit, with the TCP protocol on the destination computer. It also provides error checking.

TCP takes messages received from the Application layer and breaks them down into smaller chunks, called **segments**, numbering and sequencing each segment so that the TCP protocol on the receiving end can resequence the segments and reassemble the message to present to the Application layer. TCP on the sending computer sends groups of packets determined by the window size, receives acknowledgment for segments received at the destination, and retransmits those that are not acknowledged. All of this comes at a price in the area of **performance**, a measurement of the operation, function, and effectiveness of a system. For that reason, there is an alternate host-to-host protocol, the User Datagram Protocol.

User Datagram Protocol

Like TCP, the User Datagram Protocol (UDP) takes an Application layer message and breaks it down into numbered segments to be reassembled by the UDP protocol on the destination computer. But it is not concerned with the order in which the segments are received at the destination, nor does it wait for acknowledgment and resend lost segments. It also does not create a virtual circuit. It just sends the segments. Any reliability or error checking is done by protocols at other layers.

Using UDP saves a great deal of network overhead. For traffic that does not require the guaranteed delivery and error tracking of TCP, the lighter, faster UDP is the answer. SNMP traffic is a good example of this. The traffic between an SNMP console and the SNMP agents on hundreds of network devices could severely degrade overall network performance if it used TCP as its connection protocol.

Real-Time Transport Protocol

The Real-Time Transport Protocol (RTP) is a Network layer protocol used in transmitting real-time audio and video. RTP does not guarantee real-time delivery of the data, only the mechanisms for sending and receiving real-time data over connectionless networks. RTP uses dynamic UDP ports that are negotiated by the sender and receiver for each media stream. The ITU-TH.323 standard for voice and video services over data networks uses RTP for transferring the audio and video data. This combined implementation of standards is included in the Microsoft videoconferencing software **NetMeeting**.

Network Layer Protocols

At the network layer, a host is identified by a logical address, the segments of the Transport layer are broken into packets, and the routing of these packets is performed. This layer also "**abstracts**," or shields, the upper-layer protocols and applications from needing to have any knowledge of the network below this layer. The Network layer understands logical addresses that define individual computer, or host, addresses and the logical subnets on which the hosts reside.

Internet Protocol (IP)

The Internet Protocol (IP) is by far the most important protocol of the Network layer. The version in place at the time Windows 2000 was released was Internet Protocol version 4 (IPv4). This has been the basis of IP and related protocols since 1981. All other protocols at this layer work with IP.

IP is a packet-switching protocol that uses logical addresses: one portion of the address indicates the logical subnet, while the other indicates the individual host on that subnet. A routing protocol selects the appropriate route for a packet. It is a connectionless protocol, and IP packets are often referred to as datagrams. An IP packet, or datagram, contains both the source and the destination addresses, in addition to the data.

Internet Protocol Version 6 (IPv6)

IPv4 has been the foundation of the TCP/IP protocol implementations since 1981. However, with the fast-depleting pool of IP addresses, there is a need to better support the varieties of traffic on both the Internet and intranets. The IETF has been working for several years on a new standard, Internet Protocol version 6 (IPv6). Beginning in the mid-1990s, the authors of this book encountered articles about this developing standard with promises that it would be introduced "within a year." Although there are some special implementations of IPv6, such as Internet2, and many vendors are including IPv6 support in their products, IPv6 has not been rolled out to the Internet, nor widely used in private corporations. We will not join the host of writers who have attempted to predict the timing of the implementation of IPv6.

IPv6 solves the depleting-address-pool problem with a new 128-bit addressing scheme that will give us the benefit of hierarchical IP addresses, much as we now have a hierarchical naming structure in DNS. It will also include security at the IP level and better support for real-time delivery of packets (QoS). Stay tuned.

Note

There is a faster Internet. It is Internet2, a consortium of government agencies, universities, and businesses involved with research (déjà vu?). The goals of Internet2 are to:

- Create a leading-edge network capability for the national research community
- Enable revolutionary Internet applications
- Ensure the rapid transfer of new network services and applications to the broader Internet community

This list is from the Internet2 informational site at www.internet2.edu.

Routing Protocols

Routing is a very important function performed at the Application layer, using the logical addresses and protocols of the Network layer. At this layer, routing involves connecting different logical networks and transmitting packets between networks.

Routing protocols can be grouped into two categories: Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). IGPs are used within an **autonomous system (AS)**, which is defined as a collection of networks, connected by routers. The routers within an autonomous system are administered by the same authority and most often use the same IGP for sharing routing information and maintaining their route tables within the AS. An example of an autonomous system would be all the corporate networks served by a single ISP. EGPs are used to communicate between autonomous systems, allowing different networks to communicate.

Windows 2000 supports no EGPs, only IGPs. In Windows 2000 routing is enabled, and routing protocols are installed and configured through the routing and remote access console in the Administrative Tools menu. Routing protocols automate administrative tasks, making it possible for routers to generate valid lists of routes without human intervention and with minimal administrative configuration. The routing protocols listed for IP routing include Open Shortest Path First (OSPF), RIP version 2 for Internet Protocol (RIPv2), the Network Address Translation Protocol (NAT), the Internet Group Management Protocol (IGMP) Version 2, and the DHCP Relay Agent. Windows 2000 also supports RIP for IPX. Below are descriptions of OSPF and RIP; the other protocols will be described later in this book.

Open Shortest Path First

Open Shortest Path First (OSPF) is a **link-state** IGP routing protocol. Link-state routing is a method of dynamic routing in which routing information is discovered by communications between routers. A router running a link-state protocol establishes neighbor relationships with other routers in its AS, then exchanges information about its network interfaces. After they exchange the link-state information, they each run an algorithm to build a logical topology map of the network. (OK, if you must know, it is Dijkstra's SPF algorithm.) This information is used to build the 'routing table'. This entire process is referred to as 'convergence'. When finished, the network is said to be converged.

The primary advantage of OSPF is that it is not as prone to routing loops as distance vector routing protocols are, and after convergence, it only exchanges a very small "hello" packet between neighbors every 30 seconds, rather than its entire routing table. When a link changes, the other routers are only sent an update for that link, rather than the entire routing table. The initial neighbor discovery is done via a reserved multicast address instead of a broadcast address. The other primary advantage is that it is a classless protocol that understands VLSM (Variable Length Subnet Mask). Only new information is transmitted. It is more efficient and has less overhead than the Routing Information Protocol (RIP). OSPF also adds load balancing and class-of-service routing.

Note

Detailed information on classless IP addressing and VLSM appears in Chapter 4.

Tip

To learn more about Dijkstra's SPF algorithm, go to www.freesoft.org/CIE and do a search on "Dijkstra."

Routing Information Protocol

The Routing Information Protocol (RIP) is a distance-vector dynamic routing protocol that is very easy to configure and maintain. The RIP protocol sends out its routing table and listens for other RIP broadcasts. Each RIP router adds 1 to the hop count of each route in the list of routes it receives from another router. These broadcasts occur at an interval, such as one minute. The problem is that each RIP router broadcasts its entire route table, creating a lot of network traffic.

RIP is probably the most widely used. It is based on a Xerox design from the 1970s. Ported to TCP/IP when LANs first appeared in the early ‘80s, RIP has changed little in the past decade and suffers from several limitations, some of which have been overcome with RIP-2, which is not discussed here. RFC 1058 documents RIP.

BootP

The BootP protocol was originally designed to enable diskless workstations to boot up on a network and broadcast a special request for an IP address and a boot image file. This request would contain the MAC address of the client (NIC physical address). A BootP server, hearing this request, would verify the MAC address, issue an IP address, and provide the boot filename and location, made available to the client by way of TFTP. BootP has been enhanced to include the present DHCP standard, now supporting Microsoft Windows 2000 client installation via Remote Installation Services (RIS).

Internet Control Message Protocol

The Internet Control Message Protocol (ICMP), a companion protocol or extension IP, defines packets that contain error, control, and information messages used for managing, testing, and monitoring the network. IP hosts and routers can report errors and exchange limited control and status information. This is the protocol used by the **Packet Internet Groper (PING)** command to test a network connection.

Internet Group Management Protocol

The Internet Group Management Protocol (IGMP) is responsible for the management of IP multicast group membership. Hosts use the IGMP protocol to request to join or leave a multicast group. IGMP is typically implemented on switches, while special multicast routing protocols, such as Distance Vector Multicast Routing Protocol (DVMRP), are implemented in the routers.

A host group can span IP routers across multiple network segments. This configuration requires IP multicast support on IP routers and the ability for hosts to register themselves with the router. Host registration is accomplished using IGMP.

Address Resolution Protocol

Packets on a TCP/IP network carry the source and destination logical addresses, known as IP addresses. These addresses are actually used in routing the packet to the subnet on which the host resides. If the sending host determines that the destination host is on its same subnet, then the sending host must resolve the logical IP address to the physical, MAC, address.

The Address Resolution Protocol (ARP) handles the logical to physical address resolution. The ARP protocol can perform a broadcast on the local subnet requesting the MAC address of the host computer holding the IP address in question (the destination address). The ARP protocol on the destination computer will respond with its MAC address.

The ARP protocol also maintains a cache in memory of IP to MAC address mappings that it has discovered in this manner. Therefore, it will first check this cache before actually sending a broadcast. Once the MAC address is discovered, the packet is sent to the destination computer. In cases in which the IP protocol on a source host discovers that the destination address is not on the local subnet, the packet must be sent to the default gateway (router). In that case, the IP address of the default gateway is known, but the MAC address of the default gateway must be discovered.

The ARP protocol goes into action to resolve the logical address to physical address, first checking its cache to see if there is an entry for the default gateway IP to MAC address resolution. Once the MAC address of the default gateway is resolved, the packet is sent to the default gateway. At the default gateway, the destination IP address is once again examined to see if it is on a subnet to which the router is directly connected. If it is, the packet is sent to the appropriate interface, where ARP is used to resolve the IP address to the MAC address of the destination host on the local subnet. If the destination IP address is not on a subnet local to the router, then IP will consult its routing table to determine which route will best reach the destination subnet.

Reverse Address Resolution Protocol

As its name implies, the Reverse Address Resolution Protocol (RARP) is the opposite of ARP. It is used when the physical, MAC, address is known, and the logical address needs to be discovered. Previous to Windows 2000, this protocol was used most often in diskless workstation implementations. In Windows 2000 Remote Installation Services (RIS), clients use RARP.

Chapter Summary

- This chapter reviewed networking basics. We assumed that you have a working knowledge of the implementing and administering a Microsoft Windows 2000 network infrastructure course or that you have passed Microsoft exam 70-216. You need to understand these numerous technologies, which were built on decades of computer network standards and development. The main reason you need this understanding is because Microsoft exam 70-221, for which you may be preparing, assumes a detailed knowledge of these technologies. This review also ensures that we have a common vocabulary as we move together through this book to study the Windows 2000 network infrastructure design process.

- We first briefly touched on the evolution of modern networks, moving from simple computer/terminal connections through LANs, MANs, and WANs. We explored the OSI reference model and touched on other models upon which current network standards are based. (We are aware that some people feel that many textbooks and computer courses beat the OSI model to death. But it truly is the basis for modern network design, and clearly understanding its interrelationships allows you to more easily understand other network models. Besides, Microsoft expects you to really know it!) We also focused on OSI peer-to-peer communication.

- We then moved into various Physical and Data Link layer protocols and technologies. We explored the transmission media, hardware, and related protocols used to connect network resources and to define how computers are linked together. We spent extra energy and time on listing network standards for OSI layers 1 and 2, which together form the basis that supports the rest of the protocol structure. These lower-layer infrastructure elements are, in most cases, already in place in the networks you will be working with. Therefore, you must not only know how it works, you also must be able to recognize when it needs to be expanded or replaced with newer technology.

- We then explored the various network connectivity models. You will most likely find yourself working with complex networks that use several different connectivity models simultaneously, and you will need to understand the similarities and differences between them.

- We also spent time with our good friends TCP and IP, which have become the bedrock protocols upon which many critical services depend. In fact, you will find that much of the work of a network designer revolves around TCP/IP, and so this chapter reviewed most of the TCP/IP protocols and services that are available in Windows 2000.

- We then examined a lengthy list of Process and Application layer protocols and services, both for review purposes and to ensure that we share a common vocabulary so that we can all move forward with minimal misunderstandings.
- The topic of network infrastructure design is enormously complicated, with many different ways of accomplishing a desired goal. There are many competing and complimentary protocols, services, products, goals, political environments, budgets, and deadlines that create a tangled web for you to cut through. We hope this book will help you through the maze (to mix some metaphors).

Key Terms

abstract — A document that summarizes a longer, more detailed document.

aggregate — A collection of somewhat similar things into one mass.

Application layer — The seventh layer of the OSI reference model. This layer contains the services that give the user access to network resources. The user initiates client access through a user application, which in turn makes a request through the Application layer. Application layer services are often implemented through the use of an Application Programming Interface (API).

Application Programming Interface (API) — A set of interfaces (now frequently in the form of an Object Model) that a software company publishes so that third parties can develop custom extensions to their software.

asynchronous — A communications method that does not depend on strict time constraints and in which data streams can be broken by random intervals.

Asynchronous Transfer Mode (ATM) — A network technology that transfers data in *cells* or packets of a fixed size. The ATM cells are relatively small compared to those used with older technologies so the small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.

autonomous system (AS) — A group of routers under the same administration often using the same Internal Gateway Protocol (RIP or OSPF).

availability — The presence of a network service to provide supported services when needed. To provide a high level of availability, as in 24 hours a day, seven days a week, every day of the year (24/7/365). Availability is now frequently expressed in uptime percent of a year; for example, "five nines" means 99.999%.

baseband — In network communications, baseband media can carry only one signal at a time.

bridge — A Data Link layer network device that physically segments a network using the same access method, but allows the segments to appear as one segment to Network layer protocols.

broadcast — In a TCP/IP network, a traffic type, sent from a single host, in which the destination address of a packet is a special broadcast address. Every device that sees this broadcast packet will process it up through the protocol layers.

Data Link layer — Protocols at this layer of the OSI model create, transmit, and receive frames. This layer uses physical addresses. The layer is actually divided into two sublayers: the Logical Link Control sublayer and the Media Access Control sublayer.

DoD Model — A four-layer model of protocols roughly combining some of the OSI reference model layers. The layers are Process/Application, Host-to-Host, Internet, and Network Access.

Exchange 2000 — The Active Directory-integrated version of the Microsoft electronic messaging server, introduced in October 2000.

extranet — Refers to an intranet that is partially accessible to authorized outsiders. Although an intranet usually resides behind a firewall and is accessible only to members of the same organization, an extranet allows various levels of accessibility to outsiders if they have a valid user name and password, and their identity determines which parts of the extranet they can view. Extranets are becoming a very popular means for business partners to exchange information.

File Transfer Protocol (FTP) — Both a protocol and its companion service that make file transfer possible between computers using TCP/IP.

frame — A packet of transmitted information.

full-duplex — Refers to the transmission of data in two directions simultaneously. For example, a telephone is a full-duplex device because both parties can talk at once. In contrast, a walkie-talkie is a half-duplex device because only one party can transmit at a time.

hub — A network device that operates at the Physical layer, serving as both a signal repeater and a central connection point for several network devices.

integrated services digital network (ISDN)—A standard for telecommunications that includes the ability to transmit voice, data, and video signals over the same media.

Internet — The worldwide network made up of many interconnected networks utilizing public communications lines and the TCP/IP protocol suite.

intranet — A private network that makes information and services available using Internet technologies, such as web servers, web browsers, FTP servers, e-mail, and newsgroups.

isochronous — Time dependent. Used to describe communications methods that depend on delivery within a specific time period. Data streams, such as multimedia, require an isochronous transport method so that data are delivered as fast as they are displayed and the audio is synchronized with the video.

link-state — An algorithm used by the Open Shortest Path First (OSPF) routing protocol in which routers send information to other routers about their direct links. Each router then calculates routes based on this information learned from other routers.

local area network (LAN) — A computer network at its simplest consists of a group of two or more computers linked together to communicate and share network resources, such as files, programs, or printers. In a LAN, networked computers are physically close to one another, often in the same building or on the same office campus.

Logical Link Control (LLC) — A sublayer at the top of the Data Link layer, defined in IEEE 802.2. Includes flow control and management of connection errors.

MAC address — A unique address contained in ROM on every network interface device.

Media Access Control (MAC) — A sublayer of the OSI Data Link layer.

metropolitan area network (MAN) — Connected LANs that span a city or metropolitan area.

mobile worker — A person who performs his or her work from various locations, using a computer to access resources on the company network, send and receive corporate e-mail, and transmit data to company servers.

multicast — A TCP/IP network traffic type in which the packets are addressed to a special group of hosts, defined as a multicast group.

NetMeeting — Software that provides real-time network-based conferencing, including multipoint data conferencing, text chat, whiteboard, and file transfer, as well as point-to-point audio and video.

Network layer — The layer 3 protocol of the OSI reference model; provides the logical addressing scheme for the network, uniquely identifying devices across the network.

network media — The physical cables linking computers in a network.

news server — A server hosting a newsgroup application.

newsgroup — An Internet application that allows users to connect to a server (news server) and read and post articles.

Open Systems Interconnect (OSI) reference model — A theoretical model, created many years ago by the International Organization for Standardization (ISO), which defines a layered network model in which protocols at each layer have a defined set of responsibilities in network communications between hosts.

packets — A message is usually broken down into these smaller pieces for easier transmission over a network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called *datagrams.*

Packet Internet Groper (PING) — A TCP/IP utility used to test connectivity. It sends packets to addresses, using the ICMP echo request, requesting the packets be echoed back to the source.

packet switching — A common communications method that divides messages into packets and sends each packet individually. Each packet may take different routes and may arrive at the destination out of order. The Internet is based on a packet-switching protocol, TCP/IP. Packet switching differs from circuit switching (the most common communications method), in which a dedicated circuit or channel is established for the duration of a transmission. The best-known circuit-switching network is the telephone system, which links together wire or fiber-optic segments to create a single unbroken line for each telephone call. Circuit-switching systems are best when data must be transmitted in real time. Packet-switching networks are more efficient if some amount of delay is acceptable.

performance — A measurement of the operation, function, and effectiveness of a service. Often related to how fast things happen.

Physical layer — The bottom, or layer, of the OSI reference model. It includes the media that carries the signals and the physical devices for network connection and control.

point-to-point — A connection between two locations using a communications carrier's network.

Post Office Protocol (POP) — A protocol used to send and retrieve e-mail from a mail server. Most e-mail applications use the POP protocol, although some can use the newer Internet Message Access Protocol (IMAP). There are two versions of POP in use today. The first, called *POP2,* became a standard in the mid-80s and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

Presentation layer — The Presentation layer of the OSI reference model is where formatting of the data, and any necessary data conversion, is done. In addition, it handles data compression, data encryption, and data stream redirection.

protocol — In networking, this is a set of rules for communicating between systems.

protocol stack — A logical layering of protocols, as defined in the OSI reference model and the DoD model.

Quality of Service (QoS) — A networking term that specifies a guaranteed throughput level.

redundancy — Removing a "single point of failure" for one component or class of components can provide fault tolerance redundancy. In networking, having multiple servers offer the same service can provide redundancy, and multiple routers can give access to the same subnet.

remote access — A network model that allows users located physically at a distance from the network to access the network, using either a dial-in connection or a virtual private network (VPN) connection.

remote office — A network model that describes a network designed to connect one or more remote segments of the organization with the organization's network. This model could involve using technologies associated with other models.

resolver — A DNS client computer, which sends requests to DNS servers in order to resolve DNS names to IP addresses.

router — Network layer device that connects segments, transmitting packets between segments based on the logical (Network layer) network address. Routers have their own specialized protocols that aid in selecting the best path for packets to travel.

security — Security as applied to networks has many meanings. These include privacy, which means other people can't see your data; integrity, which means other people can't change your data; authentication, which means you know someone is who they say they are; nonrepudiation, which means that when someone completes a transaction, they can't go back and claim it never happened; and prevention of denial of service.

segment — A physical portion of a network.

Session layer — The Session layer of the OSI reference model manages the session between two computers, working to establish, synchronize, maintain, and end each session. Authentication, connection ID, data transfer, acknowledgments, and connection release are performed by the protocols at this layer.

switch — A device that combines the capabilities of a hub and a bridge, going beyond the multiport repeater capabilities of a hub by routing based on MAC address.

synchronous — Usually used to describe communications in which data streams can be delivered only at specific regular intervals.

Synchronous Optical NETwork (SONET) — A high-speed Physical layer protocol standard for MAN technology using fiber-optic cable.

T-carrier system — A system developed by Bell Telephone Laboratories to multiplex voice signals onto digital transmission lines. Customers buy all or a portion of the T-carrier capabilities. The levels of service include T-1 at 1.544 Mbps, and fractional T-1 that provides a portion of the T-1 bandwidth.

Time Division Multiple Access (TDMA) — A multiplexing method used on SONET networks that divides broadband communications channels into separate time slots in order to allow more data to be carried simultaneously.

Token Ring network — A physical star but logical ring network standard developed by IBM, using the token-passing access method.

topology — The physical layout of transmission media and the logical method for transmitting data, mapping to the Physical and, usually, Data Link layers of the OSI reference model.

Transmission Control Protocol/Internet Protocol (TCP/IP) — A widely used protocol suite for routed networks, which includes many more protocols than the two used to identify it.

Transport layer — The Transport layer of the OSI reference model is responsible for error and flow tracking, dividing outgoing messages into smaller segments and reassembling incoming messages.

unicast — In a TCP/IP network, a unicast packet is addressed to a single host.

virtual private network (VPN) — The encapsulation or "tunneling" of packets between end points over a network for security.

web browser — The client software of the World Wide Web that allows users to browse for Web servers and display the content.

web servers — The servers, located on an intranet or the Internet, that provide graphical content accessed by client computers using special web browser software that can interpret and display the content.

wide area network (WAN) — A network of networks connected across large geographical areas, even spanning continents and oceans.

Review Questions

1. What are the three fundamental network types, based on geographical scope of the network?
   a. bus, ring, star
   b. LAN, MAN, WAN
   c. bridge, router, gateway
   d. SONET, X.25, ATM
2. What organization designed the OSI reference model?
   a. ARPANET
   b. Internet
   c. IEE
   d. ISO
   e. ITU
3. At what layer of the OSI reference model does packet routing occur?
   a. Data Link
   b. Presentation
   c. Network
   d. Session
4. Which layer of the OSI reference model understands the physical address of a NIC?
   a. Network
   b. MAC sublayer of the Data Link layer
   c. Physical
   d. Session
5. Which of the following topologies needs to be terminated to avoid signal bounce?
   a. mesh
   b. star
   c. ring
   d. bus
   e. hybrid
6. Which of the following topologies provides the most redundancy?
   a. mesh
   b. star
   c. ring
   d. bus
   e. hybrid

7. Which of the following best describes the topologies you are likely to encounter in a corporation today?
   a. mesh
   b. star
   c. ring
   d. bus
   e. hybrid
8. Which of the following has an access method that can result in signal collisions?
   a. Token Ring
   b. ArcNet
   c. intranet
   d. Ethernet
9. The IEEE 802 committees decided that one of the layers of the OSI reference model needed to be divided into two sublayers. Which layer was this?
10. Which WAN technology that can be used for LAN implementations uses cell switching rather than packet switching of other more common WAN technologies?
11. What is the fastest speed at which Ethernet networks can operate?
12. Which of the following would be considered for a network backbone for a large corporate Intranet?
    a. FDDI
    b. X.25
    c. ISDN
    d. RS-232
13. Which of the following would you consider for the backbone of a large enterprise network (select all that apply)?
    a. ATM
    b. ISDN
    c. 16 Mbps Token Ring
    d. FDDI
    e. 100 Mbps Ethernet
14. What are the five network connectivity models that may be included in a Windows 2000 network infrastructure design?
15. What term describes two computers that have a connection over a switched network?
    a. T-carrier
    b. asynchronous connection
    c. virtual circuit
    d. ISDN connection

16. As a network designer, you need to provide remote access connections for a sales force that works out of their homes. What types of connections are you most likely to consider?
    a. fiber optic or ATM
    b. routed connection
    c. dial-up, ISDN, or DSL
    d. leased line
17. What network device would be needed to connect a remote office to an organization's intranet?
    a. router
    b. punch-down block
    c. MAU
    d. CAU
    e. none of the above
18. You need to provide Internet access for three to four users in a sales office. What is your most logical solution?
19. The corporate office of 50 users needs Internet access for moderate to heavy use. What is the most practical connection option?
    a. a shared modem connection
    b. a dedicated T-carrier line connected to an ISP
    c. individual dial-up connections
    d. a cellular connection
    e. none of the above
20. NewArk Widgets needs to connect their intranet to the networks of each of their suppliers. They will be connected through one or more routers. What is the name for this type of network model?
    a. intranet
    b. WAN
    c. extranet
    d. LAN
    e. all of the above
21. For what is synchronous communications used?
    a. e-mail
    b. client/server applications
    c. time-critical data
    d. network server administration

22. Unbreakable AutoGlass needs to give access to their mobile sales force. Each person has a notebook computer and dial-up access to the Internet. You have decided to allow them access to the corporate intranet through the Internet. How can you make this a secure connection?

    a. select Callback in the User properties in Active Directory

    b. set up a VPN for each salesperson

    c. have the users connect through Hotmail

    d. have the users delete the temporary Internet files on their notebooks

23. What is the act of forwarding packets, based on logical address, from one subnet to another?

24. What Internet layer protocol of the TCP/IP suite is used by the PING utility?

    a. IP

    b. ARP

    c. ICMP

    d. IGMP

25. What Internet layer protocol of the TCP/IP suite is used to resolve logical addresses to physical addresses?

    a. ICMP

    b. IGMP

    c. RARP

    d. ARP

HANDS-ON PROJECTS

Project 1-1 Research the International Organization for Standardization (ISO)

In this hands-on activity, you use the Internet to research the International Organization for Standardization (ISO). This organization plays a major role in establishing international standards for many types of organizations. In this chapter you learned that the ISO designed the Open Systems Interconnect (OSI) reference model.

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the Security Dialog box titled Log on To Windows.
3. In the User Name box, type **administrator**.
4. In the Password box, type **password**. (If this does not work, ask your instructor for the password.)

5. In the Log on To box, use the selection arrow to select **INTERSALES**. (This, too, will depend on the classroom configuration).
6. Press **Return** or click the **OK** button.
7. When the desktop appears, double-click the **Internet Explorer** button on the desktop.
8. In the Address box, type **http://www.iso.ch**. The home page of the ISO will appear in the browser.
9. Research the following questions: What is the origin of ISO? What is the official start date of the ISO? What is the stated objective of the ISO? Record your answers in a lab book or a word-processed document.
10. Exit the site and close down your browser.

Project 1-2 Research the Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is a group concerned with solving the technical challenges of the Internet with standard solutions so that the Internet can continue to function as a vendor-independent, worldwide entity. In this project you will research the workings of the IETF.

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the Security Dialog box titled Log on To Windows.
3. In the User Name box, type **administrator**.
4. In the Password box, type **password**. (If this does not work, ask your instructor for the password.)
5. In the Log on To box, use the selection arrow to select **INTERSALES**. (This, too, will depend on the classroom configuration.)
6. Press **Return** or click the **OK** button.
7. When the desktop appears, double-click the **Internet Explorer** button on the desktop.
8. In the Address box, type **http://www.ietf.org**. The home page of the Internet Engineering Task Force will appear.
9. Explore the answers to the following questions: Where is the actual work of the IETF accomplished? What is the title of the manager of one of these entities? What is the name of the group to which this manager belongs? What is the name of the oversight group and what does it do? What document, with a curious name (to which there is a link), is recommended to "first time attendees?" Record your answers in a lab book or a word-processed document.
10. Exit the site and close down your browser.

Project 1-3 Search for a Numbered Request for Comment (RFC) Document

The IETF maintains the Request for Comment (RFC) documents and makes them available on their web site. You may need to read an RFC to better understand a protocol or service you are considering using in your network design. The following will help you through a search for a document when you know the appropriate RFC number.

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the Security Dialog box titled Log on To Windows.
3. In the User Name box, type **administrator**.
4. In the Password box, type **password**. (If this does not work, ask your instructor for the password.)
5. In the Log On To box, use the selection arrow to select **INTERSALES**. (This, too, will depend on the classroom configuration.)
6. Press **Return** or click the **OK** button.
7. When the desktop appears, double-click the **Internet Explorer** button on the desktop.
8. In the Address box, type **http://www.ietf.org**. The home page of the Internet Engineering Task Force will appear in the browser.
9. On the IETF home page, click the **RFC Pages** link. This will bring you to the Request for Comments page.
10. On the Request for Comments page under IETF repository retrieval, enter the number **792** in the box for RFC number. Record the title in a lab book or a word-processed document. Click the **back arrow** on the toolbar of the Internet Explorer window to return to the IETF RFC page.
11. On the RFC page, enter the number **2328** in the box for RFC number. Record the title in a lab book or a word-processed document.
12. Exit the site and close down your browser.

Project 1-4 Search for a Named Request for Comment (RFC) Document

There will be times when you need to learn more about a protocol or service you are considering for a design. You know the name, but you do not know the RFC number. In this project you will locate documents relating to the Dynamic Host Configuration Protocol.

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the Security Dialog box titled Log on To Windows.
3. In the User Name box, type **administrator**.

4. In the Password box, type **password**. (If this does not work, ask your instructor for the password.)
5. In the Log on To box, use the selection arrow to select **INTERSALES**. (This, too, will depend on the classroom configuration.)
6. Press **Return** or click the **OK** button.
7. When the desktop appears, double-click the **Internet Explorer** button on the desktop. In the Address box, type **http://www.ietf.org**. The home page of the Internet Engineering Task Force will appear in the browser.
8. On the IETF home page, click the **RFC Pages** link. This will bring you to the Request for Comments page.
9. On the Request for Comments page, scroll down to the bottom and click the **RFC Editor Web Pages** link.
10. On the RFC Editor page, click the **RFC Search and Retrieval** link.
11. On the page titled "Searching and Retrieving RFCs from the RFC Editor Site," notice that there are several options for searching for RFCs. Use the link you found to locate RFCs that pertain to the Dynamic Host Configuration Protocol. Record your answers in a lab book or a word-processed document.
12. Exit the site and close down your browser.

Project 1-5 Discover the MAC Address of a Local Network Card

You may need to discover the MAC (physical) address of a computer's network card. In this project you will use the IPCONFIG command to examine the IP configuration and discover the MAC address of a network card. This is a good method when you have direct access to a computer.

1. Log on to Windows 2000.
2. Click the **Start** button on the desktop.
3. Highlight **Programs**, and then highlight **Accessories**. (If Accessories and other menus are not displayed, click the up or down chevrons to view the Program menu's contents.)
4. Click **Command Prompt**.
5. At the command prompt, enter the command **IPCONFIG/ALL**.
6. The output from this command shows you the IP configuration of all network adapters in this computer, including NICs, modems, and other network connection devices.
7. Type **exit** to close the command prompt window.

Project 1-6 Discover the MAC Address of a Remote Network Card

Sometimes you need to discover the MAC (physical) address of a remote machine. The following is a method in which you use the Ping and ARP commands to discover a remote computer's MAC address. You'll need the name of another computer on your network to finish this project.

1. Log on to Windows 2000 and click the **Start** button on the desktop.
2. Highlight **Programs**, and then highlight **Accessories**. (If Accessories and other menus are not displayed, click the up or down chevrons to view the Program menu's contents.)
3. Click **Command Prompt**.
4. At the command prompt, enter the command **PING *computername*** where *computername* is the name of the computer you recorded above.
5. If the Ping command is successful, the output from this command shows that the four packets sent to the computer have been returned. In order to send packets to another computer on your subnet, your computer needed to first resolve the computer name to a logical address (the IP address), and resolve that address to a physical address. The ARP protocol is responsible for this last task. It holds recently resolved names in its cache (the ARP cache) for a short period of time. The protocol also has a companion command line program, ARP, which allows you to view the contents of the ARP cache. You may view this cache, if you are fast enough.
6. From the command prompt, type **arp –a**. The result of this command will be the display of all the physical addresses that have been resolved and the logical addresses that map to them.
7. Type **exit** to close the command prompt window.

CASE PROJECTS

Case 1-1 Expanding an Existing Network

You are a member of the network group for ZYX Company. They have recently acquired the CBA Company. The intranet at the ZYX corporate headquarters campus consists of 1,000 client computers and 50 servers. The client subnets are running on 10 Mbps Ethernet, while the backbone, where the servers reside, is running on 100 Mbps Ethernet. Network performance has been an issue for some time. You are now faced with adding the 500 additional computers and 12 additional servers of CBA Company to the Ethernet network at the headquarters of ZYX. The network group has formed a task force to plan for the network expansion.

1. Describe how using switches would allow ZYX to keep the present cabling in place, but effectively provide more bandwidth. What are the pros and cons?
2. What would be the pros and cons of upgrading the entire LAN to 100 Mbps Ethernet without adding switches?
3. Describe the pros and cons of adding switches to solution 2.
4. Can you give yet another solution and the possible pros and cons?

Case 1-2 Researching Gigabit Ethernet (for Teams)

You are a consultant with the Pretty Good consulting firm. You are currently "on the bench," meaning between assignments. You have been asked to work with another consultant to create and deliver a presentation on the various options to migrate a corporate LAN from Ethernet to 1,000 Mbps Ethernet (Gigabit Ethernet). Together, you and your partner will research possible solutions using the Internet or other resources you discover. Write a summary of your discoveries, which should cover the following questions:

1. Why is there so much interest in Gigabit Ethernet?
2. What is the expected life of a cabling infrastructure?
3. Name some cable options for Gigabit Ethernet.
4. What are the benefits of migrating to Gigabit Ethernet?
5. What about using the existing Category 5 cable?
6. Name and describe a new standard for Category 5 cable.
7. Is special hardware required?
8. Who manufactures equipment and cable for Gigabit Ethernet?
9. Can the migration be evolutionary or must it be revolutionary?
10. What are the disadvantages of migrating to Gigabit Ethernet?

To find answers to these questions, a good place to start is at the web sites for such vendors as 3Com, Intel, and Cisco. Other sources are magazines, such as *Windows 2000* magazine, found at www.winntmag.com, and phone company web sites, such as www.bell-atl.com, which is now part of Verizon. The Gigabit Ethernet Alliance has information on the status of standards to support Gigabit Ethernet: They can be found at www.gigabit-ethernet.org.